COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Version 29 septembre 2017
Strasbourg, France

T-CY (2017)2

Comité de la Convention sur la cybercriminalité (T-CY)

Rapport d'évaluation sur l'entraide judiciaire : suites données par les Parties et Observateurs

Projet préparé par le Bureau du T-CY par examen par la T-CY 18
(27-28 novembre 2017)

www.coe.int/TCY

Contents

1 Contexte 4

2 Suites données par les Parties aux Recommandations 1 à 15 7

2.1 Rec 1 – Mise en oeuvre des dispositions de la Convention de Budapest 7
2.1.1 Bilan des suites données 7
2.1.2 Exemple de bonnes pratiques 7
2.1.3 Conclusion 7
2.2 Rec 2 – Statistiques et suivi de l'efficience de l'entraide judiciaire 8
2.2.1 Bilan des suites données 8
2.2.2 Exemples de bonnes pratiques 8
2.2.3 Conclusion 9
2.3 Rec 3 – Allocation de ressources 10
2.3.1 Bilan des suites données 10
2.3.2 Exemples de bonnes pratiques 10
2.3.3 Conclusion 11
2.4 Rec 4 – Formation pour l'entraide judiciaire 12
2.4.1 Bilan des suites données 12
2.4.2 Exemples de bonnes pratiques 13
2.4.3 Conclusion 14
2.5 Rec 5 – points de contact 24/7 14
2.5.1 Bilan des suites données 15
2.5.2 Exemples de bonnes pratiques 16
2.5.3 Conclusion 16
2.6 Rec 6 – Rationaliser les procédures d'entraide judiciaire 17
2.6.1 Bilan des suites données 17
2.6.2 Exemples de bonnes pratiques 17
2.6.3 Conclusion 18
2.7 Rec 7 – Utilisation de tous les canaux 18
2.7.1 Bilan des suites données 18
2.7.2 Exemples de bonnes pratiques 19
2.7.3 Conclusion 19
2.8 Rec 8 – Emergency procédures 19
2.8.1 Bilan des suites données 19
2.8.2 Exemples de bonnes pratiques 20
2.8.3 Conclusion 20
2.9 Rec 9 – Accusé de réception et notification de l'action entreprise 21
2.9.1 Bilan des suites données 21
2.9.2 Exemples de bonnes pratiques 21
2.9.3 Conclusion 22
2.10 Rec 10 – Ouverture d'investigations au niveau national 22
2.10.1 Bilan des suites données 22
2.10.2 Exemple de bonnes pratiques 23
2.10.3 Conclusion 23
2.11 Rec. 11 – Transmission électronique des demandes 24
2.11.1 Aperçu général des suites données à la Recommandation 24
2.11.2 Exemples de bonnes pratiques 24
2.11.3 Conclusion 24
2.12 Rec. 12 – Demandes spécifiques contenant toutes les informations nécessaires 25
2.12.1 Aperçu général des suites données à la Recommandation 25
2.12.2 Exemples de bonnes pratiques 25
2.12.3 Conclusion 26
2.13 Rec. 13 – Flexibilité dans l'application des normes de double incrimination 27
2.13.1 Aperçu général des suites données à la Recommandation 27
2.13.2 Exemples de bonnes pratiques 27
2.13.3 Conclusion 29
2.14 Rec. 14 – Consultation préalable 30
2.14.1 Aperçu général des suites données à la Recommandation 30

2.14.2 Exemples de bonnes pratiques....30
2.14.3 Conclusion....32
2.15 Rec. 15 – Transparence au sujet des conditions applicables, des seuils et des motifs de refus..33
2.15.1 Aperçu général des suites données à la Recommandation....33
2.15.2 Exemples de bonnes pratiques....33
2.15.3 Conclusion....34
3 Période de conservation des données (Rec. 16)....35
3.1 Durée de la période de conservation....35
3.2 Aperçu général des suites données à la Recommandation....39
3.3 Conclusion....40
4 Recommandations 17 et 18....41
4.1 Rec. 17 – Formulaires plurilingues....41
4.1.1 Suites données à la Recommandation....41
4.1.2 Conclusion....41
4.2 Rec. 18 – Ressources en ligne....42
4.2.1 Suites données à la Recommandation....42
4.2.2 Conclusion....42
5 Conclusions, recommandations et suivi....43
5.1 Conclusions....43
5.2 Recommandations....43
5.3 Suivi....47
6 Annexe : Suites données à la Recommandation du T-CY sur l'entraide judiciaire à travers des activités de renforcement des capacités....49

Contact
Alexander Seger
Secrétaire exécutif du Comité de la Convention sur la cybercriminalité (T-CY)
Direction générale des Droits de l'homme et de l'État de droit
Conseil de l'Europe, Strasbourg, France
Tél +33-3-9021-4506
Fax +33-3-9021-5650
Email: alexander.seger@coe.int

1 Contexte

L'entraide judiciaire rapide est l'une des conditions les plus importantes préalables à l'efficience des mesures de lutte contre la cybercriminalité et d'autres infractions impliquant des preuves électroniques, puisque ce type de preuve est par nature transnational et volatil. Or, dans la pratique, les procédures d'entraide judiciaire sont, dans certaines circonstances, jugées trop complexes, trop longues et trop gourmandes en ressources, ce qui les rend de ce fait par trop inefficientes.

Le Comité de la Convention sur la cybercriminalité (T-CY), à sa 8e Session plénière (5-6 décembre 2012), a donc décidé d'évaluer en 2013 l'efficience de certaines dispositions du chapitre III de la Convention de Budapest sur la cybercriminalité concernant la coopération internationale, et notamment l'article 31 qui prévoit une entraide judiciaire rapide pour ce qui est de l'accès à des données stockées au moyen d'un système informatique :

> Article 31 – Entraide concernant l'accès aux données stockées
> 1 Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, et de divulguer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conserves conformément à l'article 39.
> ...
> 3 La demande doit être satisfaite aussi rapidement que possible dans les cas suivants :
> a) il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification ; ou
> b) les instruments, arrangements et législations évoqués au paragraphe 2 prévoient une coopération rapide.

L'évaluation s'est conclue par l'adoption du Rapport d'évaluation par la 12e Plénière du T-CY les 2-3 décembre 2014[1].

Le Rapport comprend un ensemble de recommandations sur des éléments relevant de la responsabilité des Parties:

Rec 1	Les Parties devraient mettre pleinement en œuvre et appliquer les dispositions de la Convention de Budapest sur la cybercriminalité, y compris pour ce qui est des pouvoirs en matière de conservation (suite au Rapport d'évaluation 2012 du T-CY).
Rec 2	Les Parties devraient envisager de tenir des statistiques ou d'établir d'autres mécanismes pour suivre l'efficience du processus d'entraide judiciaire en ce qui concerne la cybercriminalité et la preuve électronique.
Rec 3	Les Parties devraient envisager, pour l'entraide judiciaire, d'affecter du personnel et du personnel plus formé aux technologies de l'information, non seulement au niveau central, mais aussi dans les institutions responsables de l'exécution des demandes d'entraide (comme les bureaux locaux des procureurs).
Rec 4	Les Parties devraient envisager de dispenser une meilleure formation pour renforcer l'entraide, la coopération policière et d'autres formes de coopération internationale en matière de cybercriminalité et de preuves électroniques. La formation et l'échange d'expérience devraient en particulier viser les procureurs et les juges et encourager une coopération directe entre autorités judiciaires. Une telle formation devrait être soutenue par les programmes de consolidation de capacités du Conseil de l'Europe et d'autres organisations.
Rec 5	Les Parties et le Conseil de l'Europe devraient travailler à renforcer le rôle des points de contact

[1] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c

	24/7 conformément à l'article 35 de la Convention de Budapest, notamment : a. à veiller, conformément à l'article 35.3 de la Convention de Budapest, à disposer de personnel formé et équipé pour faciliter le travail opérationnel et conduire ou soutenir des activités liées à l'entraide ; b. à veiller à ce que les points de contact promeuvent activement leur rôle auprès des autorités nationales et de leurs homologues étrangères ; c. à assurer entre les Parties des réunions régulières et la formation du réseau 24/7 ; d. à encourager les autorités compétentes et les points de contact 24/7 à envisager des procédures de suivi pour superviser le traitement des demandes basées sur l'article 31 et à faire un retour d'information à l'État requérant ; e. à établir, dans la mesure du possible, des points de contact (supplémentaires) dans les services de poursuite pour permettre un rôle plus direct en matière d'entraide et une réponse plus rapide aux demandes ; f. à faire jouer aux points de contact 24/7 un rôle de soutien dans les demandes « article 31 ».
Rec 6	Les Parties devraient envisager de rationaliser les procédures et de réduire le nombre d'étapes requises pour les demandes d'entraide au niveau national. A cet égard, les Parties doivent partager les bonnes pratiques avec le T-CY.
Rec 7	Les Parties devraient utiliser tous les canaux disponibles pour la coopération internationale. Ceci peut inclure l'entraide judiciaire formelle, la coopération policière et d'autres.
Rec 8	Les Parties sont encouragées à établir des mesures d'urgence pour des demandes liées au risque pour la vie et à des circonstances extrêmes similaires. Le T-CY devrait documenter les pratiques des Parties et des fournisseurs de services.
Rec 9	Les Parties devraient accuser réception des demandes systématiquement et notifier, sur demande, les actions prises.
Rec 10	Les Parties devraient envisager l'ouverture d'une enquête nationale sur demande étrangère ou information spontanée pour faciliter le partage d'information ou accélérer l'entraide.
Rec 11	Les Parties devraient utiliser la transmission électronique des demandes conformément à l'article 25.3 de la Convention de Budapest relatif aux moyens rapides de communication.
Rec 12	Les Parties devraient veiller à ce que les demandes soient spécifiques et contiennent toutes les informations nécessaires.
Rec 13	Conformément à l'article 25.5 de la Convention de Budapest et au Paragraphe 259 du Rapport explicatif, les Parties sont encouragées à faire preuve de flexibilité lorsqu'elles appliquent la double incrimination pour faciliter l'octroi de l'aide.
Rec 14	Les Parties sont encouragées à consulter les autorités de la Partie requise avant d'envoyer les demandes, quand cela est nécessaire.
Rec 15	Les Parties devraient assurer la transparence en ce qui concernant les conditions applicables en matière de demande d'entraide, et les raisons d'un refus, notamment pour les seuils concernant les affaires vénielles, sur les sites web des autorités centrales.

Les Parties avaient été invitées à donner suite aux recommandations relevant de leur responsabilité et à faire rapport au T-CY dans les 18 mois sur les mesures prises afin que le T-CY puisse, conformément à son Règlement intérieur (Article 2.1.g), évaluer les progrès accomplis.

A la suite d'une décision de la T-CY 15 (24-25 mai 2016) d'inviter le Bureau à élaborer et le Secrétariat à diffuser une demande d'information sur les suites données aux Recommandations 1 à 7 et 9 à 15 du Rapport d'évaluation de l'entraide judiciaire, ainsi qu'à la Recommandation 16 sur la durée pour la conservation des données, un questionnaire préparé par le Bureau du T-CY a été

diffusé à toutes les Parties le 16 septembre 2016, l'échéance pour les réponses étant fixée au 21 octobre 2016. A cette date, 18 Parties y avaient répondu.

La T-CY 16 (14-15 novembre 2016) a décidé d'accueillir avec satisfaction les réponses des 18 États Parties au questionnaire et d'inviter les États Parties et Observateurs ne l'ayant pas encore fait à y répondre pour le 15 décembre 2016.

La T-CY 17 (7-9 juin 2017) a décidé d'inviter les Parties et Observateurs à faire part de leurs commentaires et d'encourager les Parties et Observateurs n'ayant pas encore répondu à renvoyer leurs réponses au Secrétariat pour le 15 juillet 2017 afin que le Bureau puisse examiner le projet de rapport sur les suites données au rapport sur l'entraide judiciaire en vue d'une discussion détaillée par la T-CY 18 (novembre 2017).

Le Bureau du T-CY a dépouillé les observations reçues et préparé un rapport consolidé à sa réunion du Bureau du 18 septembre 2017 pour examen par le T-CY.

Au 17 juillet 2017, 40 États Parties et 1 État Observateur avaient répondu au questionnaire :

Albanie	Finlande	Pays-Bas
Arménie	France	Norvège
Australie	Allemagne	Philippines
Autriche	Hongrie	Pologne
Azerbaïdjan	Israël	Portugal
Belgique	Italie	Roumanie
Bosnie-Herzégovine	Japon	Serbie
Bulgarie	Lettonie	Slovaquie
Canada	Liechtenstein	Slovénie
Croatie	Lituanie	Espagne
République tchèque	Malte	Suisse
Danemark	Ile Maurice	Turquie
République dominicaine	Moldova	États-Unis d'Amérique
Estonia	Monténégro	

2 Suites données par les Parties aux Recommandations 1 à 15[2]

2.1 Rec 1 – Mise en œuvre des dispositions de la Convention de Budapest

Les Parties devraient pleinement mettre en œuvre et appliquer les dispositions de la Convention de Budapest sur la cybercriminalité, y compris les pouvoirs en matière de conservation des données (suite au rapport d'évaluation de 2012 du T-CY).

2.1.1 Bilan des suites données

Cette Recommandation était issue du fait que les Parties pensaient que la pleine application des dispositions de coopération internationale et procédures déjà inscrites dans la Convention de Budapest serait d'une grande aide pour obtenir des preuves dans un contexte international.

La plupart des États ayant répondu au questionnaire affirment qu'ils sont en conformité avec les exigences de la Convention[3]. Certains précise spécifiquement que leur droit contient une disposition établissant la conservation (Albanie, Arménie, Australie, Canada, Croatie, Finlande, Japon, Lettonie, Lituanie, Malte, Moldova, Monténégro, Pays-Bas, Norvège, Philippines, Pologne, Portugal, Roumanie, Slovaquie, Espagne, États-Unis)[4].

Certains États qui ne disposent pas de disposition légale établissant la conservation s'appuie sur des compétences implicites permettant d'ordonner la conservation (Bulgarie, République tchèque, Estonie, France). D'autres envisagent actuellement d'inscrire une telle disposition dans les textes législatifs ou réglementaires (Azerbaïdjan, Italie, Slovénie).

Un petit nombre d'États exigent une entraide judiciaire formelle pour répondre aux demandes de conservation article 29, voire ne sont pas pleinement conformes avec la Convention (Hongrie, Ile Maurice et Turquie)[4]. D'autres sont en train d'améliorer leur mise en œuvre de la Convention au niveau national[5] (Bosnie-Herzégovine, République tchèque, Liechtenstein et Serbie).

2.1.2 Exemple de bonnes pratiques

De nombreux États appliquent la bonne pratique consistant à inscrire une disposition relative à la conservation dans leur droit interne qui permet d'exécuter simplement et rapidement la mesure de conservation sans ordonnance judiciaire.

2.1.3 Conclusion

---

[2] Note : Le Bureau des Programmes du Conseil de l'Europe sur la cybercriminalité (C-PROC) en Roumanie soutient les États Parties et Observateurs dans leur mise en œuvre de la Convention de Budapest grâce à toute une palette de projets et d'activités, notamment dans les suites données aux recommandations du Rapport du T-CY sur l'entraide judiciaire. Ces activités ne sont pas énumérées spécifiquement pour chaque Recommandation. Une liste des projets figure en annexe au présent rapport.

[3] Chypre, la Géorgie, l'Islande, le Luxembourg, Panama, le Sri Lanka, «l'ex-République yougoslave de Macédoine», l'Ukraine, et le Royaume-Uni n'ont pas répondu à cette question.

[4] Pour une analyse détaillée de la mise en œuvre des dispositions liées à la conservation, voir les rapports T-CY Assessment report Implementation of the preservation provisions of the Convention de Budapest on Cybercrime https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e722e
Assessment Report: Implementation of the preservation provisions of the Convention de Budapest on Cybercrime : supplementary report
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168044be2b

Les dispositions procédurales et de coopération internationale dans la Convention de Budapest sont cruciales pour l'obtention de preuves au niveau international et devraient être pleinement mises en œuvre. En particulier, la conservation est de tous l'outil le plus basique, le plus fréquemment utilisé et le moins intrusive. Les Parties devraient lever les obstacles à l'utilisation facile des pouvoirs de conservation et envisager sérieusement d'inscrire des dispositions relatives à la conservation sous la forme contraignante (loi, règlement ou autre) appropriée à leur pays.

2.2 Rec 2 – Statistiques et suivi de l'efficience de l'entraide judiciaire

> Les Parties devraient envisager de tenir des statistiques ou d'établir d'autres mécanismes pour suivre l'efficience du processus d'entraide en ce qui concerne la cybercriminalité et les preuves électroniques.

2.2.1 Bilan des suites données

Par cette Recommandation, les Parties suggéraient que des données concrètes sur la charge croissante que représentent les demandes de preuve électronique – mieux que des réclamations générales – pourraient alerter les décideurs politiques et peut-être débloquer plus de ressources pour les bureaux qui traitent les demandes d'entraide judiciaire impliquant des données électroniques.

Bon nombre d'États tiennent des statistiques concernant les demandes d'entraide judiciaire concernant des données électroniques[6] et pourraient consulter des bases de données existantes pour obtenir ces statistiques, ou disposent de nouveaux systèmes de gestion des documents et des affaires qui permettent la tenue de statistiques (Albanie, Australie, Azerbaïdjan, Belgique, Bulgarie, Canada, Croatie, Hongrie, Italie, Lituanie, Malte, Ile Maurice, Moldova, Monténégro, Roumanie[7], Serbie, Slovaquie, Slovénie, Espagne, Suisse, Turquie, États-Unis). D'autres sont en train de développer des systèmes de ce type (Bosnie-Herzégovine, République tchèque, Finlande, Pays-Bas).

Certains États affirment que la tenue de statistiques n'existe pas ou n'est pas possible (Arménie, Autriche, Danemark, France[8], Israël, Liechtenstein, Norvège, Pologne). Au Liechtenstein, le nombre des affaires est suffisamment petit pour que l'efficience puisse être évaluée sans base de données.

Le Portugal a relevé, et l'Allemagne aussi, qu'il est impossible de tenir des statistiques exactes sur les demandes d'entraide judiciaire impliquant des données électroniques car la coopération directe entre autorités judiciaires ne passe pas par des points de contrôle centraux. La coopération directe est largement citée comme outil d'amélioration de la cyber-coopération et est très utilisée entre les États membres de l'UE.

2.2.2 Exemples de bonnes pratiques

Australie : l'Autorité centrale tient une base de données de toutes les affaires ayant donné lieu à une demande d'entraide judiciaire, y compris en matière de cybercriminalité et pour des preuves électroniques. Cela lui permet de produire des statistiques sur le nombre d'affaires par catégories

[6] Chypre, la Géorgie, l'Allemagne, l'Islande, la Lettonie, le Luxembourg, Panama, le Sri Lanka, « l'ex-République yougoslave de Macédoine », l'Ukraine et le Royaume-Uni n'ont pas répondu à cette question. Cette note de bas de page était prévue pour suppression. Faute d'explication et étant donné que la majeure partie des notes de bas de page similaires n'étaient pas marquées pour suppression, elle a été conservée.

[7] Roumanie – par le biais du bureau du procureur durant l'enquête – conserve des statistiques uniquement pour l'entraide judiciaire sur la cybercriminalité, pas pour celles sur les preuves électroniques.

[8] La France peut suivre le nombre d'affaires traitées par l'Autorité centrale mais pas spécifiquement le nombre d'affaires concernant la cybercriminalité et les preuves électroniques.

(notamment par pays d'origine, type d'infraction et type d'assistance). L'Autorité centrale examine actuellement ses critères pour la gestion des affaires en vue de créer une base de données améliorée. Elle suit également en permanence et analyse les pratiques en matière de gestion des affaires pour ce qui est de la réactivité et l'efficience.

Canada : l'Autorité centrale conserve une base de données électroniques de toutes les demandes d'entraide judiciaire demandant des données électroniques émanant du Canada ou qui lui ont été adressées ; cette base de données identifie la nature de l'infraction sous-jacente, le type d'assistance demandé et les données traitées. Elle permet aussi de télécharger tous les documents et correspondance associés à la demande pour s'y référer facilement.

Malte : le Bureau du Procureur général a une base de données qui conserve des informations statistiques sur toutes les demandes entrantes et sortantes d'entraide judiciaire, notamment celles concernant des cyber-délits et des preuves électroniques.

Moldova: Le Bureau du Procureur général tient des statistiques sur toutes les demandes d'entraide judiciaire, y compris concernant la cybercriminalité. Avec le Service de l'Informatique et de la lutte contre la cybercriminalité, il suit strictement les demandes liées à la cybercriminalité.

Monténégro : l'Autorité centrale utilise un logiciel électronique de gestion des affaires pour l'entraide judiciaire, qui permet d'obtenir des données statistiques selon différents critères tels que l'infraction pénale, le type d'entraide judiciaire ou encore l'État requérant.

Philippines : le ministère de la Justice des Philippines – Service de la cybercriminalité (DOJ-OOC) tient fidèlement des registres/bases de données des demandes d'entraide judiciaire entrantes et sortantes concernant la cybercriminalité et la preuve électronique.

Suisse : des statistiques sont publiées en ligne (liens fournis).

États-Unis : l'Autorité centrale tient une base de données pour toutes les demandes d'entraide judiciaire entrantes qui demandent des enregistrements électroniques (que la demande soit parvenue en version papier ou électronique). La base de données suit, entre autres, la durée de traitement d'une demande, les communications de et vers l'État requérant, et la résolution de chaque affaire. Le système peut également produire des statistiques et des tendances concernant ces types de demande.

2.2.3 Conclusion

Il semble que la plupart des États sont en mesure de produire des statistiques sur les demandes d'entraide judiciaire impliquant des données électroniques. Il serait intéressant de voir si ces statistiques reflètent l'impression exprimée par les praticiens de la lutte contre la cybercriminalité – à savoir que le système est lent et surchargé. Au-delà de ça, le T-CY pourrait analyser si des statistiques agrégées pourraient être utilisées d'une manière ou d'une autre. Il serait utile de partager les statistiques disponibles avec le T-CY[9].

Il peut être intéressant de voir si d'autres États qui peuvent s'appuyer sur des contacts directs rencontrent le problème soulevé par le Portugal, à savoir que cela empêche les États de tenir des statistiques précises.

[9] Note : Durant l'évaluation par le T-CY, très peu d'États parties ont fourni des données statistiques.

2.3 Rec 3 – Allocation de ressources

> Les Parties devraient envisager, pour l'entraide, d'affecter davantage de personnel et du personnel plus formé aux technologies, non seulement au niveau central mais aussi au niveau des institutions responsables de l'exécution des demandes (comme les Bureaux locaux des procureurs).

2.3.1 Bilan des suites données

L'idée derrière cette Recommandation était que l'entraide judiciaire peut être ralentie voire échouer si les agents de la chaîne de l'entraide judiciaire ne connaissent pas la technologie en question dans une affaire – ils risquent de ne pas poser la bonne question ou de ne pas fournir le bon fondement pour soutenir ou accélérer une demande d'entraide judiciaire.

De manière générale, les Parties prennent au sérieux les problèmes sous-jacents à cette Recommandation. La plupart les traitent, essentiellement par la formation, la liaison et l'organisation d'équipes de spécialistes[10]. Les trois approches sont souvent combinées.

Les États ci-dessous sont classés globalement selon les grands points qu'ils ont mis en avant dans leurs réponses. Cela ne veut pas dire pour autant qu'ils ne prennent pas d'autres mesures. Au contraire, il semble que les États testent différentes méthodes pour diffuser et approfondir les connaissances techniques.

Les Parties signalent spécifiquement :

- la formation pour les agents travaillant sur des demandes d'entraide judiciaire impliquant des données électroniques : Australie, Belgique, Bulgarie, Finlande ;
- le travail en réseau ou des liens spéciaux entre services pertinents, par exemple entre les bureaux de procureur qui traitent des demandes d'entraide judiciaire impliquant des données électroniques et la cyber-police nationale : Autriche, République dominicaine, Allemagne, Hongrie, Liechtenstein, Malte, Slovaquie ;
- équipes de personnel spécialisé : Albanie, Azerbaïdjan, Canada, République tchèque, Danemark, Estonie, France, Israël, Japon, Lituanie, Ile Maurice, Moldova, Norvège, Roumanie, Suisse, Turquie, États-Unis.

D'autres États analysent actuellement ce problème, et mettent l'accent sur la formation spécialisée dans les services locaux du parquet, ou le recrutement de personnel spécialisé sur le plan technique (Bosnie-Herzégovine, Finlande, Pologne, Serbie).

2.3.2 Exemples de bonnes pratiques

Australie : l'Autorité centrale forme ses praticiens à leur entrée en poste puis en formation permanente pour qu'ils se tiennent à niveau concernant les technologies émergentes et la manière dont les criminels s'en servent.

Autriche : la coopération entre les procureurs et la cyberpolice dans les services centraux de la police est rapide, souple et efficiente. De plus, au niveau régional, chaque tribunal et service de procureur dispose de personnel technique qui peut l'appuyer.

[10] La Croatie, Chypre, la Géorgie, l'Islande, le Luxembourg, Panama, le Sri Lanka, « l'ex-République yougoslave de Macédoine », l'Ukraine et le Royaume-Uni n'ont pas répondu à cette question. Le Portugal a indiqué qu'aucune mesure spécifique n'a été prise.

Azerbaïdjan : du personnel spécialisé en informatique est affecté au traitement des demandes d'entraide judiciaire impliquant des données électroniques tant aux niveaux centraux que dans les institutions responsables de l'exécution des requêtes.

Canada : création récente d'une Unité Cyber au sein de l'Autorité central canadienne pour relever le niveau d'expertise cyber, conserver du personnel spécialisé en informatique et mettre en œuvre un processus permettant d'accroître l'efficience et d'assurer la cohérence dans l'analyse et l'exécution des requêtes demandant l'accès à des données électroniques. Les membres de cette Unité reçoivent une formation permanente dispensée par des experts cyber.

France : dans de nombreux services de l'administration française (notamment au sein de l'Autorité centrale et à Paris, Lille et ailleurs), il y a des magistrats, des praticiens et des unités dédiées spécialistes de la cybercriminalité, de la collecte de preuves électroniques, de l'informatique forensique et des cyber-investigations.

Israël : le Bureau du Procureur public dispose d'un Service international qui sert d'autorité désignée pour les questions de droit et de technologie, et d'un Service de lutte contre la cybercriminalité. Ce dernier rencontre régulièrement des homologues étrangers ainsi que plusieurs fournisseurs de services sur Internet.

Japon : dans le Service des Procureurs suprêmes et dans les Bureaux des procureurs de district de première importance, des procureurs formés aux nouvelles technologies sont chargés des affaires de cybercriminalité. Le ministère de la Justice promeut également la capacité des membres des services de poursuite à enquêter sur des affaires de cybercriminalité dans tout le pays en dispensant des formations sur les technologies utilisées dans la cybercriminalité et sur les méthodes d'enquêtes électroniques. Au sein des forces de police nationales et préfectorales, les enquêtes dans des affaires de cybercriminalité sont confiées à du personnel spécialisé dans les nouvelles technologies.

Lituanie : les demandes d'entraide judiciaire impliquant des données électroniques sont traitées conjointement par des procureurs et des enquêteurs chevronnés connaissant très bien les problématiques techniques et juridiques. Le recueil technique de la preuve est traité par des cyber-enquêteurs affectés à des divisions chargées de la lutte contre la cybercriminalité soit au niveau central de la police nationale, soit au niveau de l'une des dix brigades policières au niveau locale. La division au niveau national chargée de la lutte contre la cybercriminalité traite normalement des affaires très en vue, concernant la criminalité organisée et des affaires transnationales.

Suisse : des unités spécialisées sur la cybercriminalité ont été établies au sein des bureaux des procureurs au niveau fédéral et cantonal. Le Bureau du Procureur Général de la Suisse compte aussi des procureurs spécialisés, ce qui garantit que les connaissances juridiques et technologiques appropriées sont disponibles pour le traitement de demandes d'entraide judiciaire impliquant des données électroniques. Il existe plusieurs plateformes pour assurer le transfert de connaissances spécialisées au sein d'un même canton et entre les autorités cantonales et fédérales.

États-Unis : dans le cadre de son projet de modernisation de l'entraide judiciaire, l'Autorité centrale américaine dispose d'une Unité cyber dont les attorneys et l'équipe de soutien se concentre exclusivement et en permanence sur les demandes d'entraide judiciaire impliquant des données électroniques. L'Autorité centrale collabore avec des procureurs dans tous les États-Unis spécialisés dans les enquêtes cyber et qui l'aident à exécuter les demandes d'entraide.

2.3.3 Conclusion

Il reste, certes, beaucoup à faire mais les États s'efforcent semble-t-il sérieusement d'accroître le niveau de formation technologique des agents chargés du traitement des demandes d'entraide judiciaire.

2.4 Rec 4 – Formation pour l'entraide judiciaire

> Les Parties devraient envisager de dispenser une meilleure formation pour renforcer l'entraide, la coopération policière et d'autres formes de coopération internationale en matière de cybercriminalité et de preuves électroniques. La formation et l'échange d'expériences devraient en particulier viser les procureurs et les juges et encourager une coopération directe entre autorités judiciaires. Une telle formation devrait être soutenue par les programmes de consolidation de capacités du Conseil de l'Europe et d'autres organisations.

2.4.1 Bilan des suites données

Le volume des requêtes internationales de preuve électronique ne faisant qu'augmenter, les Parties avaient recommandé une formation plus spécialisée, dispensée à un maximum de praticiens. Les Parties pensaient que cela accélérerait l'entraide judiciaire et rendrait le processus plus efficient.

Les Parties semblent s'attaquer avec sérieux à la mise en œuvre de cette recommandation, en s'y prenant de différentes manières[11].

De nombreux États ont des établissements de formation pour les policiers, les procureurs et les juges. Dans ces établissements, certains ont intégré ou sont en train de développer des formations régulières ou occasionnelles :

- sur les connaissances générales en cyber ainsi que sur les demandes d'entraide judiciaire impliquant des données électroniques (Azerbaïdjan, Belgique, Bosnie-Herzégovine, Bulgarie, Croatie, République tchèque, Danemark, Italie, Japon, Lettonie, Lituanie, Moldova, Roumanie, Serbie, Slovaquie, Suisse, États-Unis) ;
- sur les demandes d'entraide judiciaire impliquant des données électroniques (Albanie, Estonie, Portugal) ;
- sur les connaissances générales en cyber (France, Monténégro, Pays-Bas, Norvège).

Un cours sur les connaissances générales en cyber n'est certes pas la même chose qu'un cours sur les demandes d'entraide judiciaire impliquant des données électroniques, cependant toute augmentation des connaissances techniques aidera à traiter ces demandes.

D'autres États assurent des formations sur un des thèmes ou les deux par des moyens autres qu'une académie ou établissement de formation officiels (Australie, Autriche, Canada, Hongrie, Ile Maurice, Slovénie, Espagne).

Certains se disent intéressés à bénéficier d'une formation ou envisagent/prévoient de le faire par eux-mêmes (République dominicaine, Finlande, Pologne).

Les données relevant de la juridiction américaine sont au cœur de bon nombre de demandes d'entraide judiciaire. C'est la raison pour laquelle diverses agences américaines, dont l'Autorité centrale, le FBI et la Section du Département d'État de la Justice chargée des infractions informatiques et de la propriété intellectuelle forment au maximum leurs partenaires étrangers

[11] Chypre, la Géorgie, l'Islande, le Luxembourg, Panama, le Sri Lanka, « l'ex-République yougoslave de Macédoine », l'Ukraine, et le Royaume-Uni n'ont pas répondu à cette question.

pour l'obtention de preuves électroniques auprès des États-Unis. Ces formations, qui se déroulent aux États-Unis, en-dehors ou par vidéoconférence, visent les juges, les procureurs et la police. De plus, les États-Unis participent à la formation dispensée par le GLACY, l'Organisation des États d'Amérique, l'Office des Nations-Unis contre la drogue et le crime et d'autres organisations.

D'autres États relevant aussi que leur formation se concentre en partie sur la manière d'obtenir des données relevant de la juridiction américaine.

Bon nombre indiquent qu'ils participent à des formations dispensées par des organisations multilatérales, dont le Conseil de l'Europe.

2.4.2 Exemples de bonnes pratiques

Belgique : une session d'initiation et une session avancée sur la cybercriminalité sont dispensées chaque année, avec une part de formation à l'entraide judiciaire. Les magistrats stagiaires doivent suivre une session de trois jours sur la coopération internationale policière et judiciaire qui couvre la coopération en matière de cybercriminalité/preuve électronique. Les magistrats autres que stagiaires peuvent également suivre cette session.

République tchèque : l'Académie judiciaire organise régulièrement des formations. Chaque année, un séminaire national de formation sur l'entraide judiciaire est organisé pour tous les procureurs et juges. Une réunion de spécialistes de l'entraide judiciaire est organisée deux fois par an pour les procureurs et une fois par an pour les juges. La formation normale à l'Académie pour les juges et les procureurs comprend des séminaires portant sur la cybercriminalité, la criminalité économique et d'autres types d'infractions. Ces séminaires couvrent aussi habituellement les demandes d'entraide judiciaire spécifiques à ce type d'affaires. Les formations pour la police sont organisées aussi régulièrement et il est prévu de les intensifier et étendre, en vue de standardiser les connaissances et la pratique en matière de détection et d'investigation concernant la cybercriminalité et de partager les bonnes pratiques. Actuellement, une session de formation pour la police aboutit à la délivrance d'un certificat en examen forensique pour ceux qui réussissent l'examen de passage.

Danemark : le Collège de police est responsable de la formation professionnelle de la police, et le Directeur du Parquet de celle des procureurs. Le National Cyber Crime Center (NC3) joue un rôle central dans l'offre de formations sur la cybercriminalité pour les deux groupes. La coopération entre ces trois entités et des représentants des districts de police a abouti à une initiative, le "Programme national de lutte contre la cybercriminalité, Niveau 1" en 2015, suivi d'un programme niveau 2. Les spécialistes du NC3 suivent eux-mêmes des formations, en premier lieu sous la forme d'un programme d'initiation de trois semaines, puis d'une formation avancée obligatoire.

Les spécialistes nationaux et policiers qui ont passé avec succès les prérequis peuvent suivre des cours dispensés par le European Cybercrime Training and Education Group, l'Agence de l'Union européenne pour la formation des services répressifs ou le mastère au University College Dublin. Les policiers se voient également proposer des cours techniques en interne ainsi que des formations externes, des séminaires etc.

Lituanie : la formation et le développement professionnel font partie de la politique lituanienne en matière de cyber-sécurité. La Lituanie participe activement aux formations menées par des agents de l'UE et par d'autres États, comme le Royaume-Uni et les États-Unis. Les officiers de police participent à ces formations chaque année. Le Bureau de Police criminelle a démarré des formations spécialisées sur divers aspects de l'enquête en matière de cybercriminalité, notamment concernant l'entraide judiciaire, en 2014, destinées aux futures recrues des unités spécialisées sur a cybercriminalité dans dix commissariats de police de comté. Jusqu'à quatre fois par an, les

bureaux des procureurs de tout le pays assurent des formations liées à la cybercriminalité pour des personnels spécialisés des services répressifs et pour les autorités judiciaires. Le Bureau du Procureur général et le Bureau de la Police criminelle devraient publier bientôt des recommandations sur la cybercriminalité destinées aux procureurs qui couvriront les qualifications légales, la coopération internationale, les techniques d'enquête et d'autres thématiques connexes.

Portugal : la coopération internationale est un thème régulièrement traité pour la formation initiale et ultérieure des juges et des procureurs au Centre d'Etudes judiciaires. Des modules sur la coopération internationale sont inclus dans le programme de formation initiale, et des séminaires, des conférences et des ateliers sur divers thèmes liés à la coopération internationale sont ensuite proposés. Les juges et les procureurs sont légalement tenus d'assister à au moins deux sessions de formation par an et certains participent à des évènements sur la coopération internationale.

Roumanie et Slovaquie : ces deux pays organisent, institutionnalisent et prennent part à des programmes de formation très complets sur une grande diversité de sujets, à des conférences et à d'autres évènements pour la police, les procureurs et les juges. Ces évènements couvrent la cybercriminalité, la coopération internationale et l'obtention de preuves relevant de la juridiction américaine. Les programmes sont organisés sous les auspices des autorités nationales, avec notamment les Écoles nationales de formation de la Justice, et par de nombreuses organisations internationales, des États partenaires et des laboratoires de recherche universitaires.

Espagne : le cours de formation initiale pour les procureurs comporte deux modules spécifiques, l'un sur l'entraide judiciaire et l'autre sur la cybercriminalité. De plus, chaque unité spécialisée du Parquet tient au moins une réunion par an pour une remise à niveau des connaissances des procureurs de leurs équipes. Des sessions communes de formation pour les deux unités spécialisées sont également organisées, notamment une formation spécifique sur les outils de l'entraide judiciaire prévus par la Convention de Budapest. En outre, des activités de formation sur les deux thématiques sont aussi proposées à tous les procureurs qui souhaitent y participer. La collaboration est très fluide : les procureurs spécialisés et les juges participent à des activités de formation de la police et réciproquement, des experts de la police assurent des formations pour les procureurs et les juges. L'INCIBE, l'Institut national de la cyber-sécurité, avec le soutien d'autres entités dont l'organisation des États d'Amérique, organise des formations sur la cybercriminalité et la cyber-sécurité auxquels participant des officiers de police et des praticiens du droit de l'Espagne et des pays d'Amérique latine.

Le Bureau des Programmes du Conseil de l'Europe sur la cybercriminalité (C-PROC) en Roumanie soutient les États Parties et Observateurs grâce à toute une palette de projets et d'activités pour la mise en œuvre de la Convention de Budapest, notamment pour ce qui est du suivi de cette recommandations et d'autres du rapport du T-CY sur l'entraide judiciaire. Ces activités ne sont pas spécifiquement mentionnées dans la partie relative à chaque Recommandation. Les projets pertinents sont énumérés dans l'annexe au présent rapport.

2.4.3 Conclusion

Les États mettent de plus en plus l'accent sur la formation de toutes les catégories de personnels amenés à prendre part à la collecte et à l'échange de preuves électroniques. A mesure qu'ils poursuivent leurs efforts, ils pourraient analyser plus particulièrement à quel rythme les formations se déroulent, si elles sont proposées à suffisamment de personnel national et aux personnes appropriées, si la formation fait partie intégrante du parcours professionnel et si elle est obligatoire ou optionnelle. Autrement dit, les États devraient envisager de systématiser la formation.

2.5 Rec 5 – points de contact 24/7

Les Parties et le Conseil de l'Europe devraient travailler à renforcer le rôle des points de contact 24/7 conformément à l'article 35 de la Convention de Budapest, notamment :

a. à veiller, conformément à l'article 35.3 de la Convention de Budapest, à disposer de personnel formé et équipé pour faciliter le travail opérationnel et conduire ou soutenir des activités liées à l'entraide ;
b. à veiller à ce que les points de contact promeuvent activement leur rôle parmi les autorités nationales et leurs homologues étrangères ;
c. à assurer entre les Parties des réunions régulières et la formation du réseau 24/7 ;
d. à encourager les autorités compétentes et les points de contact 24/7 à envisager des procédures de suivi pour superviser le traitement des demandes basées sur l'article 31 et à faire un retour d'information à l'État requérant ;
e. à établir, dans la mesure du possible, des points de contact (supplémentaires) dans les services de poursuite pour permettre un rôle plus direct en matière d'entraide et une réponse plus rapide aux demandes ;
f. à faire jouer aux points de contact 24/7 un rôle de soutien pour les demandes « article 31 ».

2.5.1 Bilan des suites données

Cette Recommandation avait pour but d'encourager les initiatives concrètes qui peuvent, pour l'essentiel, être menées par les États eux-mêmes.

Dans leur presque totalité, les États prennent des mesures pour suivre la Recommandation[12], et pratiquement tous signalent qu'ils s'assurent de la disponibilité de personnel formé et équipé pour faciliter le travail opérationnel et mener ou soutenir l'exécution de demandes d'entraide judiciaire impliquant des données électroniques.

Bon nombre encouragent leurs points de contact à promouvoir leur rôle auprès d'homologues nationaux et/ou étrangers (Belgique, Bulgarie, Croatie, Danemark, République dominicaine, France, Hongrie, Italie, Japon, Lituanie, Malte, Ile Maurice, Moldova, Pays-Bas, Roumanie, Serbie, Slovaquie, Espagne, Suisse, États-Unis).

Dans certains États, les personnels concernés enseignent ou participant à des réunions et formations liées au système 24/7 soit dans leur pays, soit avec des partenaires étrangers (Belgique, Croatie, Hongrie, Italie, Lettonie, Liechtenstein, Ile Maurice, Moldova, Roumanie, Espagne, États-Unis).

Dans un petit nombre d'États, les autorités compétentes et les points de contact 24/7 élaborent ou participent à des procédures pour le suivi et le retour d'information à l'État requérant en ce qui concerne les requêtes Article 31 (Hongrie, Lituanie, Malte, Slovaquie, Espagne, États-Unis).

Un nombre significatif d'État a établi formellement ou dans les faits des points de contact dans les bureaux des procureurs (Albanie, Belgique, France, Italie, Liechtenstein, Lituanie, Malte, Ile Maurice, Pays-Bas, Roumanie, Serbie, Espagne, Suisse, États-Unis). La République de Moldova et la Pologne envisagent actuellement cette solution.

[12] Note : il a été parfois difficile de voir, les réponses étant relativement concises, quelles actions un pays avait menées ou à quelle catégorie de la question les rattacher.
Chypre, la Géorgie, l'Allemagne, l'Islande, le Luxembourg, Panama, le Sri Lanka, l'Ukraine, et le Royaume-Uni n'ont pas répondu à la question.

De même, dans un nombre significatif d'États, les points de contact 24/7 facilitent ou soutiennent le traitement des requêtes Article 31 (Arménie, Australie, Bulgarie, Canada, République tchèque, Danemark, France, Liechtenstein, Lituanie, Malte, Ile Maurice, Roumanie, Serbie, Slovaquie, Espagne, Suisse, Turquie, États-Unis).

2.5.2 Exemples de bonnes pratiques

Bulgarie : le point de contact rencontre très fréquemment différents organes des services répressifs en Bulgarie afin de promouvoir son rôle et ses capacités. Il est hébergé par l'Unité d'enquête sur les affaires de cybercriminalité de la Direction générale de lutte contre la criminalité organisée pour garantir qu'il dispose de personnel convenablement formé et de compétences et capacités nationales. Grâce à un réseau de relations informelles, il entretient de bonnes relations avec différentes organisations gouvernementales et non gouvernementales et avec le secteur privé.

France : les officiers de police très expérimentés affectés au point de contact 24/7 sont situés dans le service français spécialisé dans les enquêtes sur les crimes électroniques, ce qui facilite l'échange d'expériences pratiques. Le point de contact 24/7 est en contact direct avec l'Autorité centrale pour garantir le meilleur traitement possible des demandes d'entraide judiciaire impliquant des données électroniques. Le point de contact conseille ses homologues étrangers sur les demandes d'entraide judiciaire et met ceux-ci en contact avec l'Autorité centrale en tant que de besoin.

Lituanie : le point de contact 24/7 est l'unité spécialisée du Bureau de Police criminelle chargée de a cybercriminalité ; il sert aussi de point de contact avec Europol, les fournisseurs de services et les bureaux du parquet. Il informe sur ses activités en matière d'évènements de formation et de réunions. Il apporte souvent son assistance aux États requérants, aux unités de police nationales et aux autorités de poursuite dans le cadre des requêtes article 31 et d'autres demandes.

Roumanie: le point de contact est l'unité spécialisée sur la cybercriminalité du Parquet roumain (Direction pour les enquêtes dans des affaires de criminalité organisée et de terrorisme). Cette unité a un certain nombre de mission prévues par la loi : elle apporte une assistance spécialisée et informe sur la législation, elle ordonne la conservation immédiate de données informatiques, saisit des objets contenant des données informatiques ou des informations liées aux données sur le trafic sur requête d'une autorité étrangère compétente. De plus, elle exécute et facilite l'exécution des commissions rogatoires concernant des affaires de cybercriminalité. Pour aider le principal point de contact, un point de contact 24/7 secondaire est établi au sein de la Police nationale roumaine, à savoir le Service de lutte contre la cybercriminalité. Les deux points de contact (Parquet et Police) coordonnent étroitement leurs activités.

États-Unis: le personnel du point de contact 24/7 – la Section sur le crime informatique et la propriété intellectuelle (CCIPS), au Département d'État de la Justice, est spécialisé dans la cybercriminalité, les infractions au droit de la propriété intellectuelle, la preuve électronique et la coopération internationale. Le personnel de l'Autorité centrale est formé en matière de demandes d'entraide judiciaire impliquant des données électroniques. Le CCIPS et l'Autorité centrale travaillent ensemble en permanence. Ils assurent ou participent à de nombreuses sessions de formation chaque année pour des collègues étrangers et américains et encouragent fortement la participation au réseau 24/7. Lors de ces évènements et à d'autres occasions, les États-Unis demandent un retour d'information sur leurs processus d'entraide judiciaire.

2.5.3 Conclusion

Les États prennent un très grand nombre de mesures diverses et variées pour améliorer les relations entre les services qui traitent les demandes d'entraide judiciaire impliquant des données

électroniques. Ces mesures sont présentées de manière détaillée dans la compilation des réponses des Parties, que toutes les Parties peuvent consulter. Le T-CY recommande de se concentrer en permanence sur l'amélioration du processus. Le Conseil de l'Europe – notamment par le biais de projets en coordination avec le T-CY – devraient soutenir le partage d'expérience entre les points de contact 24/7. Une étroite coopération avec les autorités judiciaires devrait être assurée.

2.6 Rec 6 – Rationaliser les procédures d'entraide judiciaire

> Les Parties devraient envisager de rationaliser les procédures et de réduire le nombre d'étapes requises pour les demandes d'entraide au niveau national. A cet égard, les Parties doivent partager les bonnes pratiques avec le T-CY.

2.6.1 Bilan des suites données

Par cette Recommandation, les Parties donnaient un signal de leur confiance dans la capacité des États à agir sur le plan interne pour simplifier leurs procédures en matière d'entraide judiciaire sans avoir à attendre que ces changements soient demandés par traité. Les États pourraient identifier les mesures inutiles sur le plan interne, en particulier à l'ère du numérique.

La plupart des États ont indiqué qu'ils ont déjà rationalisé les procédures[13]. Pour ceux qui ont expliqué comment ils s'y étaient pris, les États ont mentionné pour l'essentiel le traitement rapide des demandes d'entraide judiciaire concernant des requêtes de preuves électroniques, l'autorisation d'un contact direct de procureur à procureur ou de juge à juge, la consultation (par exemple avec l'autorité requérante ou le service d'exécution) et/ou le recours à des procédés de communication électroniques (Australie, République tchèque, Estonie, Hongrie, Japon, Liechtenstein, Lituanie, Malte, Ile Maurice, Norvège, Roumanie, Serbie, Slovaquie, Slovénie, Espagne).

Différentes procédures ont été évoquées pour les États membres de l'Union européenne. Dans les cas appropriés au regard du traité applicable, les demandes d'entraide judiciaire entrantes sont envoyées directement à l'autorité judiciaire compétente.

L'Italie et les Pays-Bas étudient actuellement comment améliorer leurs systèmes et devraient le faire par voie législative.

2.6.2 Exemples de bonnes pratiques

Autriche : on peut accéder sur l'intranet à des informations sur les meilleures pratiques triées par pays.

Azerbaïdjan : le Bureau du Procureur général a modifié le règlement intérieur pur que les requêtes urgentes et importantes soient exécutées par des procureurs.

Belgique : auparavant, les autorisations de perquisitions et saisies étaient demandées à deux reprises dans les demandes d'entraide judiciaire – une fois avant l'exécution et une fois avant la transmission des preuves. Cette double autorisation a été abolie.

République tchèque : si un traité établit des points de contact directs entre procureurs ou juges, les procureurs ou juges concernés sont responsables de l'affaire et des communications, cependant deux autorités judiciaires centrales pour l'entraide judiciaire servent de bureau d'aide. Normalement, les services des procureurs, aux degrés inférieurs, ne communiquent qu'avec le

[13] La Croatie, Chypre, la Finlande, la Géorgie, l'Allemagne, l'Islande, le Luxembourg, Panama, le Sri Lanka, « l'ex-République yougoslave de Macédoine », l'Ukraine et le Royaume-Uni n'ont pas répondu à cette question. L'Albanie, la Bulgarie, Israël, le Portugal et la Suisse ont signalé qu'il n'y avait pas de développements récents.

bureau de niveau immédiatement supérieur. Toutefois, en matière d'entraide judiciaire, le procureur, quel que soit son niveau hiérarchique, peut contacter directement l'Autorité centrale 14. Il en va de même pour les juges tchèques : tout juge quel que soit son niveau peut contacter directement le ministère de la Justice.

Philippines : le DOJ-OOC a rédigé et proposé pour adoption la Procédure de rédaction des demandes d'entraide judiciaire relatives à la cybercriminalité et à des affaires liées à l'informatique, qui réduit le nombre d'étapes requises pour le traitement des demandes d'entraide judiciaire.

Espagne : l'Autorité centrale (ministère de la Justice) utilise pleinement les moyens de communication électroniques. Pour obtenir rapidement l'entraide judiciaire, il est important de renforcer la coopération directe telle qu'établie dans la Convention de Budapest pour les affaires urgentes. Parfois, même si l'entraide judiciaire est demandée par des moyens traditionnels (les canaux officiels) via l'Autorité centrale, les services répressifs des États requérant et requis peuvent prendre des mesures de manière non officielle avant réception de la requête officielle. Ainsi, les demandes d'entraide judiciaire américaines concernant les cyber-attaques contre SONY ont été traitées selon cette coopération directe.

États-Unis : l'Autorité centrale a établi une Unité Cyber pour traiter les entraides judiciaires concernant des preuves électroniques. Dans la mesure du possible, cette Unité exécute elle-même les requêtes sans les transférer au bureau du Procureur fédéral concerné aux États-Unis. Des attorneys de l'Unité Cyber sont en charge d'États et régions spécifiques. Ainsi, les partenaires étrangers ont un contact permanent à qui s'adresser pour les requêtes et questions.

2.6.3 Conclusion

Un petit nombre d'États ont dressé la liste des nouvelles mesures concrètes qui ont été prises. Le T-CY recommande cependant que les États continuent d'examiner l'efficacité de leurs systèmes et recherchent les étapes pouvant être supprimées, en particulier en examinant ce que les États partenaires ont fait.

2.7 Rec 7 – Utilisation de tous les canaux

> Les Parties devraient utiliser tous les canaux disponibles pour la coopération internationale. Ceci peut inclure l'entraide judiciaire formelle, la coopération policière et d'autres.

2.7.1 Bilan des suites données

Cette Recommandation reposait sur deux constats : premièrement, les canaux formels pour l'entraide judiciaire sont trop lents et toute autre méthode acceptable sur le plan légal peut être plus rapide et, deuxièmement, les canaux formels pour l'entraide judiciaire (du moins dans certains États) commencent à s'engorger du fait du volume de requêtes pour des preuves électroniques, qui explose. Tout transfert de preuve par un moyen légalement approprié effectué en-dehors des canaux formels non seulement peut se révéler plus rapide, mais peut aussi libérer du temps de traitement pour les requêtes qui ne peuvent emprunter que des canaux formels.

La plupart des États utilisent tous les canaux applicables, qu'il s'agisse des points de contact 24/7, des canaux police-police, des officiers de liaison étrangers, d'Europol, des canaux diplomatiques, d'Interpol, de l'Association internationale des procureurs, d'Eurojust, du Réseau judiciaire européen ou encore d'autres réseaux de coopération, et les canaux formels de l'entraide

[14] Ce mécanisme s'applique lorsqu'aucun contact direct n'a été établi par traité.

judiciaire[15]. Certains réponses sont explicitées ; des États relèvent qu'ils peuvent choisir un canal différent si les circonstances l'exigent (Azerbaïdjan, Croatie, France, Monténégro).

Deux États ont mentionné spécifiquement qu'ils envoient des requêtes directes à des fournisseurs de services sur internet basés aux États-Unis sans passer par les autorités américaines, comme le droit américain l'autorise (Bulgarie, Lituanie). Toutefois, d'autres sources – rapports sur la transparence des FSI par exemple – indiquent que d'autres États que la Bulgarie et la Lituanie envoient aussi des requêtes directes aux FSI américains. Apparemment, des États n'ont pas vu ce point dans leurs réponses (de nombreux États semblent avoir répondu à la Question 7 uniquement en tant qu'État requis, et n'ont pas traité le cas où ils sont requérants).

2.7.2 Exemples de bonnes pratiques

Canada : le Canada encourage l'utilisation de tous les canaux disponibles, notamment l'entraide judiciaire formelle, la coopération policière et la coopération entre autorités de poursuite. Son Autorité centrale a créé pour ses partenaires étrangers une liste des types de preuve qui peuvent être obtenues sans qu'il soit nécessaire de passer par l'entraide judiciaire formelle. Dans les formations dispensées à ses partenaires étrangers, le Canada rappelle régulièrement l'assistance qui peut être obtenue sans entraide judiciaire.

Israël : Israël a établi un "Centre national Cyber" au sein de l'Unité Cyber de la Police israélienne ainsi qu'un Service Cybercriminalité au sein du Bureau du Procureur général. Ces deux antennes facilitent activement le traitement des requêtes par des canaux non formels.

Italie : la police judiciaire facilite la coopération policière et traite les demandes d'entraide judiciaire. Il existe un protocole de communication efficace pour harmoniser et accélérer les pratiques des services de polices et du Parquet.

2.7.3 Conclusion

La plupart des États déclarent utiliser tous les canaux disponibles pour demander des informations et mettre de nombreux canaux à disposition des États leur demandant des informations. Le T-CY recommande que les canaux informels soient utilisés (et au besoin développés) au maximum autorisé par les dispositions légales applicables. Cela accélérera l'assistance et devrait aussi atténuer les engorgements dans les canaux formels.

2.8 Rec 8 – Emergency procédures

> Les Parties sont encouragées à établir des procédures d'urgence pour les demandes liées aux risques pour la vie et à des circonstances extrêmes similaires. Le T-CY devrait documenter les pratiques des Parties et des fournisseurs de service.

2.8.1 Bilan des suites données

Un petit nombre d'États ont établi des procédures d'urgence formelles ; cette recommandation visant à déterminer les procédures suivies par d'autres États.

[15] Chypre, la Finlande, la Géorgie, l'Allemagne, l'Islande, le Luxembourg, Panama, le Sri Lanka, « l'ex-République yougoslave de Macédoine », l'Ukraine et le Royaume-Uni n'ont pas répondu à cette question. L'Albanie n'a pas signalé de développements récents.

Un nombre limité d'États ont répondu complètement sur le fond à cette question16. La plupart traite seulement la manière dont ils recevraient et traiteraient des requêtes urgentes, et non s'ils sont des compétences juridiques spéciales leur permettant de fournir des preuves plus rapidement. La plupart des États n'abordent pas spécifiquement les situations de vie ou de mort.

Les réponses admettent dans leur presque totalité que des urgences surviennent en lien avec des preuves électroniques. Dans leur très grande majorité, les États déclarent qu'en cas d'urgence, leur personnel travaille plus dur, plus rapidement et alerte leurs collègues nationaux sur l'urgence de l'affaire. Il ne s'agit pas de sous-estimer l'intérêt de cette approche et de savoir gré aux personnes concernées pour les résultats qu'elle procure. Cependant, ces résultats dépendent de la diligence et de l'engagement des personnes impliquées et non d'une procédure établie et bien comprise.

Aucun État n'est doté d'une procédure bien rôdée pour les situations d'urgence couvrant toutes les catégories de données, y compris le contenu. Le droit américain permet la divulgation d'urgence de données sur l'abonné, le trafic et le contenu, mais cette disposition n'est pas obligatoire. Les fournisseurs de services sur Internet couverts par le droit américain peuvent décider de faire droit à ces demandes de divulgation ou de les refuser.

2.8.2 Exemples de bonnes pratiques

Plusieurs États indiquent qu'en général, lorsqu'une requête entrante porte la mention « Urgente », ils en tiennent compte. Il arrive aussi qu'ils réalisent par eux-mêmes qu'une requête est urgente quand bien même l'État requérant ne l'avait pas mentionné. Dans ce cas, ils traitent la requête aussi rapidement que possible (Arménie, Canada, Danemark, Estonie, Israël, Italie, Liechtenstein, Serbie, Turquie, États-Unis [si la divulgation volontaire est inapplicable]).

Bulgarie : si l'État requérant mentionne qu'une requête est urgente, il existe en vertu de la Loi sur les communications électroniques des procédures pour l'accès accéléré aux données demandées.

Lettonie : légalement, une affaire est présumée urgente lorsqu'il s'agit de prévenir ou de mettre au jour une infraction pénale, de sauver la vie d'une personne, de la protection de l'État ou de la sécurité publique. En de tels cas, plusieurs catégories de données sur l'abonné peuvent être communiquées en trois heures ou moins.

Suisse : au cas par cas, les autorités de poursuite peuvent éviter ou repousser des éléments de procédure ou conditions préalables qui peuvent ralentir le processus.

2.8.3 Conclusion

Le nombre d'affaires impliquant un danger de mort ou un risque de blessures, et où des preuves électroniques stockées à l'étranger sont cruciales, est en train d'augmenter, et rien ne permet de penser que cette tendance soit amenée à s'inverser à l'avenir. Peut-être du fait que les décideurs politiques n'ont pas conscience que le personnel opérationnel fait ce qu'il peut pour s'entraider dans des cas d'urgence, les États n'ont rien mis en place, ou peu de choses, en matière de procédures spécifiques d'urgence numérique en-dehors de faire confiance à leurs opérationnels pour se débrouiller. Le T-CY recommande que les praticiens fassent remonter la réalité de terrain aux politiques et que les États persistent au niveau national dans leurs efforts pour améliorer et formaliser les mécanismes à déclencher en cas d'urgence.

[16] La Croatie, Chypre, la Finlande, la Géorgie, la Hongrie, l'Islande, le Japon, la Lituanie, le Luxembourg, la Moldova, les Pays-Bas, Panama, le Portugal, la Slovaquie, la Slovénie, Sri Lanka, « l'ex-République yougoslave de Macédoine », l'Ukraine et le Royaume-Uni n'ont pas répondu à cette question. L'Albanie, l'Australie, l'Autriche, la France, l'Ile Maurice, le Monténégro et ma Roumanie ont renvoyé aux réponses antérieures ou n'avaient pas de nouveautés à communiquer.

2.9 Rec 9 – Accusé de réception et notification de l'action entreprise

Les Parties devraient accuser réception des demandes systématiquement et notifier, sur demande, les actions prises.

2.9.1 Bilan des suites données

Cette recommandation découle du fait que les États Parties ont signalé que souvent ils ne savent pas si une demande d'entraide judiciaire a été reçue, où en est son traitement et à qui s'adresser pour s'informer. Cette situation est particulièrement frustrante si une requête est en cours pendant des mois ou des années.

La plupart des États indiquent qu'ils prévoient sous une forme ou une autre la confirmation des demandes d'entraide judiciaire. Soit d'initiative, soit sur demande, ils notifient également les États sur la suite donnée à la requête[17].

- Plusieurs États (Australie, Estonie, Finlande, Hongrie, Italie, Liechtenstein, Malte, Norvège, Serbie, Slovaquie) assurent un accusé automatique de réception d'une demande d'entraide judiciaire. Ils informent également de leur propre chef sur la suite donnée à la requête et/ou communiquent les coordonnées de la personne à contacter qui traite l'affaire.

- D'autres assurent un accuse automatique de réception mais n'informent de l'avancée du dossier ou des coordonnées de la personne à contacter que si on le leur demande (Roumanie, Slovénie, États-Unis).

- Un grand nombre d'État confirme la réception sur demande (Arménie, Azerbaïdjan, Autriche, Belgique, Bosnie-Herzégovine, Canada, République dominicaine, Japon, Lettonie, Moldova, Monténégro, Espagne, Turquie). Pour certains, les informations sur l'avancée du dossier sont également fournies sur demande.

Deux États – la Bulgarie et la Suisse –n'ont pas de procédures de confirmation, bien que la Bulgarie travaille à s'en doter.

Dans plusieurs États Parties (Azerbaïdjan, France, Israël, Lituanie, Ile Maurice, Pays-Bas), les points de contact 24/7 accusent réception des requêtes. Certains fournissent des informations actualisées sur les mesures entreprises, soit automatiquement, soit sur demande. On ne sait pas clairement si ces réponses s'appliquent aux procédures relatives aux demandes d'entraide judiciaire ou uniquement aux requêtes reçues initialement par les points de contact 24/7[18].

2.9.2 Exemples de bonnes pratiques

Australie : dans les 2 à 5 jours ouvrés, l'Autorité centrale confirme par écrit (normalement, par mail) la réception des requêtes entrantes, et indique la référence du dossier. Une fois la requête affectée à un membre du personnel de l'Autorité centrale, celui-ci communique ses coordonnées directes de contact au requérant étranger pour faciliter les mises à jour.

[17] La Croatie, Chypre, la Géorgie, l'Allemagne, l'Islande, le Luxembourg, Panama, le Sri Lanka, « l'ex-République yougoslave de Macédoine », l'Ukraine et le Royaume-Uni n'ont pas répondu à la question. L'Albanie et Portugal n'ont communiqué aucun développement.
[18] Par exemple, le point de contact 24/7 de la France ne confirme que les requêtes pour une conservation.

Hongrie : un accusé de réception de la demande et des informations sur les grandes étapes de son traitement sont toujours communiqués au pays requérant. Lorsque la demande est transférée au Bureau du procureur concerné, une notification écrite (avec les coordonnées de la personne contact) est envoyée au pays requérant.

Liechtenstein : lorsque la requête est affectée à un juge, l'État requérant reçoit immédiatement un accuse de réception avec la cote de l'affaire et les coordonnées du juge. Il est informé du sort réservé à la demande puis se voit communiquer les preuves demandées ou la raison du refus de la requête.

2.9.3 Conclusion

La meilleure pratique est l'accusé automatique de réception des requêtes et, à mesure que l'affaire est traitée, la communication automatique des coordonnées de contact de la personne qui traite le dossier et tient le requérant au courant de son avancée. Il arrive toutefois que les États n'aient pas les ressources nécessaires pour cela. Le T-CY recommande donc que le point d'entrée pour les demandes d'entraide judiciaire – y compris le point de contact 24/7, s'il ne reçoit pas que des demandes 24/7 mais aussi demandes d'entraide judiciaire – confirme automatiquement la réception de la requête.

Les États ont donné des réponses très variées, parfois peu claires sur la facilité à obtenir concrètement les informations sur le contact et l'état d'avancement du dossier. Le T-CY souligne que les États devraient prendre toutes les mesures possibles pour que le mécanisme fonctionne sans heurts. Un État requis doit veiller à ce que l'État requérant sache à qui s'adresser pour avoir des informations sur l'avancement de l'affaire. L'Autorité centrale, un bureau du Parquet, etc. peuvent répondre à ces demandes d'informations, mais le système ne fonctionnera pas si l'État requérant ne sait pas à qui s'adresser. Enfin, la personne concernée de l'État requis doit renseigner rapidement sur l'état d'avancement de la requête à mesure que l'affaire est traitée.

2.10 Rec 10 – Ouverture d'investigations au niveau national

> Les Parties devraient envisager l'ouverture d'une enquête nationale sur demande étrangère ou information spontanée pour faciliter le partage d'information ou accélérer l'entraide.

2.10.1 Bilan des suites données

Le principal objectif de cette recommandation était que les États transfèrent les informations aussi facilement que le leur permettent les dispositions légales applicables. L'article 26 de la Convention de Budapest offre une base légale au transfert d'informations spontanées car ces informations peuvent aider un autre État à poursuivre la criminalité. De même, des preuves obtenues dans une enquête nationale peuvent aider l'enquête dans un autre État.

Une question en plusieurs éléments était posée concernant la Recommandation 10 et les États ont souvent répondu à des parties seulement de la question[19].

- De nombreux États peuvent utiliser des informations spontanées qui leur sont transmises (Arménie, Australie, Azerbaïdjan, Belgique, Canada, République tchèque, Danemark, Lettonie, Ile Maurice, Norvège, Portugal, Roumanie, Serbie).

[19] Chypre, la Géorgie, l'Islande, le Luxembourg, Panama, le Sri Lanka, l'Ukraine et le Royaume-Uni n'ont pas répondu à cette question. La Bulgarie et Israël n'avaient pas de développements à signaler.

- Une petite poignée d'États signalent spécifiquement qu'ils peuvent transmettre des informations spontanées à d'autres États (Croatie, République tchèque, Liechtenstein, Roumanie, Suisse, Turquie).

- De manière générale, les États peuvent envisager l'ouverture, ou doivent procéder à l'ouverture, d'enquêtes nationales lorsqu'un État étranger le leur demande. Des enquêtes ne sont ouvertes que si les conditions prévalant au niveau national sont respectées et si l'ouverture d'une enquête semble appropriée (Albanie, Arménie, Australie, Autriche, Belgique, Bosnie-Herzégovine, Canada, République tchèque, Danemark, Finlande, France, Allemagne, Japon, Liechtenstein, Ile Maurice, Pologne, Portugal, Roumanie, Serbie, Slovaquie20, Espagne, États-Unis).

- Un petit nombre d'États n'entame en général pas d'enquête nationale sur la base de requêtes étrangères (Lituanie, Moldova, Monténégro). La Lituanie relève que cela ne restreint pas le partage d'information ni ne ralentit l'entraide judiciaire, les enquêtes nationales n'étant pas nécessaires pour accélérer le processus d'obtention de preuves. La Moldova a ouvert une enquête de ce type concernant des preuves électroniques.

2.10.2 Exemple de bonnes pratiques

Autriche : des enquêtes nationales sont souvent ouvertes sur requête d'un État étranger.

Danemark : la possibilité [d'ouvrir une enquête nationale] est toujours examinée par l'autorité compétente pour le traitement d'une demande d'entraide judiciaire.

Allemagne : une étroite coopération est en place entre le point de contact 24/7 allemand (affecté au Bureau de la Police fédérale) et un parquet spécialité dans la lutte contre la cybercriminalité. Sur la base des informations et requêtes collectées par le point de contact 24/7, le parquet est souvent en mesure d'entamer sa propre enquête criminelle.

Norvège : une enquête nationale peut être ouverte si les faits en l'espèce de l'affaire sont liés à la Norvège. Il n'est pas nécessaire qu'un État le lui demande, les autorités norvégiennes peuvent envisager d'elles-mêmes cette option.

Serbie : sur demande, une enquête nationale est ouverte et toutes les informations pertinentes rassemblées dans ce cadre sont partagées avec les autorités étrangères.

2.10.3 Conclusion

De plus en plus, les enquêtes impliquant des preuves électroniques concernent plus d'un pays. Dans une affaire, les racines ou les victimes peuvent concerner une dizaine ou une vingtaine d'États et, sur le plan concret, les enquêteurs dans un pays peuvent radicalement réduire e temps de travail de leurs homologues étrangers s'ils partagent leurs données. Il ne ressort pas clairement de cette étude combien de fois il est recouru aux mécanismes d'information spontanée ou à l'ouverture d'une enquête nationale, et donc si ces deux formes de fonctionnement facilitent ou non l'assistance autant qu'elles le pourraient.

Le T-CY recommande que les États Parties partagent des bonnes pratiques sur l'utilisation de l'article 26 de la Convention de Budapest concernant l'information spontanée.

[20] Au Portugal, l'enquête nationale doit être ouverte à des fins nationales, non comme aide à la coopération internationale. La Roumanie et la Slovaquie ont signalé que les informations dans une demande d'entraide judiciaire peuvent être utilisées à des fins limitées seulement. C'est pourquoi il peut être nécessaire d'obtenir l'autorisation avant de se server de ces informations pour ouvrir une enquête nationale.

2.11 Rec. 11 – Transmission électronique des demandes

> Les Parties devraient utiliser la transmission électronique des demandes conformément à l'article 25.3 de la Convention de Budapest relatif aux moyens rapides de communication.

2.11.1 Aperçu général des suites données à la Recommandation

Cette Recommandation répond à la nécessité de rationaliser le processus de l'entraide judiciaire de toutes les façons possibles.

Les réponses peuvent être réparties en deux groupes. Les répondants ont indiqué en général : 1) s'ils envoient des demandes par la voie électronique, ou 2) s'ils autorisent d'autres États à le faire. Peu d'États ont répondu aux deux volets de la question.[21]

Dans de nombreux États, la transmission électronique est autorisée dans le cas des affaires urgentes, lorsqu'un État partenaire en fait la demande ou à condition que la demande électronique soit suivie par une demande sur papier (Azerbaïdjan, Belgique, Bosnie-Herzégovine, Bulgarie, Croatie, États-Unis, Japon, Liechtenstein, Lituanie, Monténégro, Pologne, République tchèque, Slovaquie, Suisse). Le Canada encourage la soumission électronique des demandes.

Certains États déclarent que la transmission électronique est possible ou fréquemment utilisée mais sans préciser si elle est utilisée à la fois pour les demandes reçues et envoyées et dans les cas non urgents (Albanie, Arménie, Australie, Autriche (« souvent utilisée »), Espagne, Estonie, Finlande, France, Hongrie, Malte, Norvège, Pays-Bas, Roumanie, Serbie).

2.11.2 Exemples de bonnes pratiques

Hongrie : les canaux de communication électronique comme le réseau SIENA d'Europol, Interpol ou le courrier électronique sont utilisés de préférence.

Malte : la télécopie, le courrier électronique et la copie papier sont utilisés.

Pays-Bas : la télécopie et le courrier électronique sont couramment utilisés.

Norvège : la pratique actuelle est l'utilisation du courrier électronique.

Serbie : les demandes reçues et envoyées sont transmises par courrier électronique suivi d'une demande sur papier.

Espagne : la télécopie et le courrier électronique sont couramment utilisés.

2.11.3 Conclusion

On voit mal pourquoi la transmission électronique des demandes ne pourrait être autorisée dans tous les cas, pas seulement dans les affaires urgentes (même si l'envoi d'une demande papier est exigé ensuite). Aucun pays n'invoque la sécurité électronique comme raison d'interdire la transmission électronique des demandes. Il se peut simplement que les États ne soient pas encore

[21] Chypre, la Géorgie, l'Allemagne, l'Islande, le Luxembourg, le Panama, le Sri Lanka, « l'ex-République yougoslave de Macédoine », l'Ukraine et le Royaume-Uni n'ont pas répondu à cette question.
L'Italie a indiqué n'avoir aucune information nouvelle à fournir à ce sujet.
Dans certains cas, en outre, il n'apparaît pas clairement si la réponse du pays porte sur les demandes 24/7 ou sur les demandes d'entraide judiciaire ; ces réponses, par conséquent, ne sont pas résumées ici.

habitués aux demandes sous forme électronique. Les États doivent réaliser, cependant, qu'avec l'augmentation du nombre des demandes, l'utilisation du papier cessera d'être pratique.

2.12 Rec. 12 – Demandes spécifiques contenant toutes les informations nécessaires

> Les Parties devraient veiller à ce que les demandes soient spécifiques et contiennent toutes les informations nécessaires.

2.12.1 Aperçu général des suites données à la Recommandation

Les États se plaignent fréquemment de l'omission d'éléments très importants – des faits matériels aux coordonnées de l'organe requérant – dans les requêtes d'entraide judiciaire et des retards inutiles qui en résultent.

La plupart des États affirment qu'ils veillent déjà à ce que leurs demandes soient spécifiques et contiennent toutes les informations nécessaires (Albanie, Australie, Autriche, Azerbaïdjan, Belgique, Bosnie et Herzégovine, Canada, Croatie, Danemark, Espagne, Estonie, États-Unis, Finlande, France, Hongrie, Japon, Lettonie, Liechtenstein, Lituanie, Malte, Maurice, Moldova, Monténégro, Pays-Bas, Portugal, République tchèque, Roumanie, Serbie, Slovaquie, Slovénie, Suisse, Turquie)22.

Plusieurs États indiquent spécifiquement que leur autorité centrale examine les requêtes avant envoi pour vérifier qu'elles sont complètes. Lorsqu'une requête doit être améliorée avant envoi, l'autorité centrale en discute avec les rédacteurs concernés (Australie, Espagne, États-Unis, France, Japon, Malte, Moldova, République tchèque, Roumanie, Serbie, Slovaquie, Turquie).

Les États mentionnent également à ce propos :

- l'organisation de formations à l'intention des différentes catégories d'agents publics chargés de préparer les requêtes d'entraide judiciaire (Belgique, Maurice, Monténégro, Pays-Bas, Slovaquie) ;
- l'existence de modèles, listes de contrôle, guides ou normes légales s'appliquant aux requêtes (Australie, Belgique, Croatie, Danemark, France, Lettonie, Maurice, Moldova, Pays-Bas, République tchèque, Serbie, Slovaquie) ;
- le travail de consultation et de liaison avec l'État requis (Canada, Estonie, États-Unis, France, Lituanie, Malte).

2.12.2 Exemples de bonnes pratiques

Australie : l'Autorité centrale utilise, pour les demandes envoyées à l'étranger, un formulaire standard qui inclut les différentes catégories d'information exigées par ses partenaires. L'autorité centrale est prête à recevoir un retour d'information sur les points spécifiques à inclure dans les requêtes envoyées par l'Australie.

France : l'Autorité centrale et les magistrats qui jouent un rôle de liaison en dehors de la France examinent les requêtes d'entraide judiciaire, y compris au moyen de consultations. La France a également produit un guide portant spécifiquement sur l'obtention de données électroniques conservées aux États Unis.

[22] Chypre, la Géorgie, l'Allemagne, l'Islande, le Luxembourg, le Panama, le Sri Lanka, « l'ex-République yougoslave de Macédoine », l'Ukraine et le Royaume-Uni n'ont pas répondu à cette question. La Bulgarie et la Norvège n'ont fourni aucune information nouvelle.

Maurice : les demandes doivent être conformes aux formats présentés dans les formations GLACY et aux normes légales mauriciennes.

Moldova : les demandes doivent inclure les éléments spécifiques énumérés dans le code de procédure pénale.

Monténégro : le centre national de formation des juges et des procureurs organise régulièrement des formations consacrées à l'entraide judiciaire à l'intention des juges et des procureurs. De plus, au moins une fois par an, le ministère de la Justice organise des réunions régionales, avec des représentants des ministères de la Justice et du système judiciaire des États avec lesquels il a conclu des accords bilatéraux, en vue d'accroître l'efficience de l'entraide judiciaire.

Slovaquie : les procureurs slovaques ont pu suivre de nombreuses sessions de formation sur l'obtention de preuves d'un pays étranger et, en particulier, des États-Unis. Il existe, à tous les niveaux du système (districts, régions, centre), des procureurs spécialisés dans la coopération internationale. Le Bureau de Procureur général leur fournit des directives. Certains de ces procureurs ont été formés conjointement avec les experts de l'Unité de lutte contre la cybercriminalité de la Direction de la police. Des activités de formation concernant les requêtes d'entraide judiciaire et, en particulier, les demandes de preuves électroniques ont également été organisées par l'Académie judiciaire à l'intention des juges et des procureurs.

Conseil de l'Europe : la Communauté Octopus sur la Cybercriminalité comprend un outil de coopération internationale, y compris un guide séquentiel pour les demandes d'entraide judiciaire portant sur des données.

2.12.3 Conclusion

D'une manière générale, les États semblent prêter une forte attention au problème des requêtes d'entraide judiciaire inadéquates. Néanmoins, les États requis continuent à se plaindre des lacunes des requêtes qu'ils reçoivent.

Les différentes méthodes décrites ci-dessus pour remédier à ces imperfections – examen par l'autorité centrale, formation, listes de contrôle, spécialisation, consultations – devraient permettre d'améliorer assez rapidement le processus de rédaction, si elles sont appliquées avec le sérieux suffisant.

Certains problèmes relatifs aux preuves électroniques sont très difficiles à résoudre ; cependant, des efforts raisonnables devraient conduire à une amélioration des requêtes.

2.13 Rec. 13 – Flexibilité dans l'application des normes de double incrimination

> Conformément à l'article 25.5 Convention de Budapest et au paragraphe 259 du Rapport explicatif, les Parties sont encouragées à faire preuve de flexibilité lorsqu'elles appliquent la double incrimination, qui faciliterait l'octroi de l'aide

2.13.1 Aperçu général des suites données à la Recommandation

L'obtention de preuves électroniques est devenue importante dans la répression de toute une gamme d'infractions pénales pour lesquelles l'aide internationale était auparavant inutile. Cette Recommandation appelle instamment les Parties à faire en sorte que les critères juridiques requis pour la transmission de preuves puissent être interprétés de manière à fournir l'aide la plus étendue possible.

La plupart des États s'efforcent de faire preuve de flexibilité dans l'application de la double incrimination, en prenant en considération les faits de l'infraction alléguée plutôt que son classement dans une catégorie d'infractions ou la terminologie employée au sens strict pour la désigner (Albanie, Arménie, Australie, Autriche, Azerbaïdjan, Belgique, Bosnie et Herzégovine, Canada, Croatie, Espagne, Estonie, États-Unis, Finlande, France, Japon, Lituanie, Malte, Maurice, Portugal, République tchèque, Roumanie, Serbie, Suisse).[23]

Plusieurs États déclarent n'avoir encore rencontré aucun cas où la double incrimination aurait justifié le refus d'octroyer l'aide judiciaire ou affirment que, bien que n'ayant pas encore rencontré le problème à ce jour, ils feraient preuve de flexibilité dans le cas où celui-ci se présentait (Albanie, Italie, Monténégro, Slovaquie).

D'autres États considèrent que le critère de double incrimination doit être respecté lorsque l'application de mesures coercitives telles que perquisition, saisie ou interception et enregistrement de télécommunications est requise (Belgique, Danemark, Norvège, Pays-Bas, République tchèque, Turquie).[24]

La République tchèque fait savoir qu'elle prévoit de retirer la réserve formulée lors du dépôt de l'instrument de ratification en relation avec l'obligation de double incrimination, de l'article 29.4 de la Convention de Budapest, pour les demandes de conservation internationales.

2.13.2 Exemples de bonnes pratiques

Canada : sauf quelques exceptions, la législation canadienne n'exige pas la double incrimination. Dans les cas bien délimités où son application est requise, le Canada fait preuve de flexibilité en se basant sur la conduite en cause, sans exiger la présence dans le droit canadien d'un équivalent exact à l'infraction étrangère.

Portugal : les autorités portugaises apportent leur coopération, même sans réciprocité, en se fondant sur la nature des faits ou sur la nécessite de combattre certaines formes de criminalité graves. Elles peuvent également le faire dans les cas où la coopération peut contribuer à améliorer la situation de l'accusé ou sa réinsertion sociale, ou à clarifier des faits se rapportant à un ressortissant portugais.

Serbie : la norme de double incrimination est appliquée de manière flexible, afin de faciliter l'octroi de l'aide. Si l'infraction pénale faisant l'objet d'une requête d'entraide judiciaire n'est pas réprimée dans le droit pénal serbe, la Serbie s'efforce, dans la mesure du possible, d'appliquer les dispositions de son code pénal visant des éléments et un mode opératoire se rapprochant le plus de l'acte décrit dans la requête.

[23] Chypre, la Géorgie, l'Allemagne, l'Islande, le Luxembourg, le Panama, la Slovénie, le Sri Lanka, « l'ex-République yougoslave de Macédoine », l'Ukraine et le Royaume-Uni n'ont pas répondu à la question. La Bulgarie a indiqué n'avoir aucun développement nouveau à rapporter en ce domaine.

[24] Pour apporter l'aide demandée, ces États peuvent, par exemple, chercher à obtenir des éléments supplémentaires du pays requérant ou offrir une forme d'aide non soumise au critère de double incrimination.

2.13.3 Conclusion

Les États déclarent qu'ils font de leur mieux pour agir avec flexibilité et s'apporter mutuellement une aide sur la base de la législation nationale et des accords internationaux. Le T-CY recommande qu'ils continuent d'évaluer la double incrimination en prenant en considération les faits de l'infraction alléguée plutôt que son classement dans une catégorie d'infractions ou la terminologie employée au sens strict pour la désigner dans la demande d'entraide judiciaire.

2.14 Rec. 14 – Consultation préalable

> Les Parties sont encouragées à consulter les autorités de la Partie requise avant d'envoyer les demandes, quand cela est nécessaire.

2.14.1 Aperçu général des suites données à la Recommandation

Cette Recommandation visait à répondre aux réclamations des Parties selon lesquelles les requêtes formelles d'entraide judiciaire imparfaites font perdre du temps à la fois à l'État requérant et à l'État requis et n'aboutissent pas au transfert de preuves. Les Parties ont souligné que des contacts très simples (appel téléphonique, courrier électronique) à un stade précoce du processus permettent de résoudre des erreurs ou des problèmes avant de consacrer du temps à une requête formelle insuffisante.

La plupart des Parties consultent l'État requis avant d'envoyer une requête formelle d'entraide judiciaire. Cette consultation préalable prend des formes diverses : envoi de questions par courrier électronique, transmission du projet de requête pour obtenir les commentaires de la Partie requise, ou envoi de questions à un agent de liaison étranger présent dans le pays. Certains États ne consultent normalement au préalable l'État requis que dans le cas d'une affaire sensible ou complexe ou lorsque cet État est un partenaire nouveau.[25]

Quelques États ne semblent pas consulter normalement l'État requis avant d'envoyer la requête (Moldova, Turquie).[26]

2.14.2 Exemples de bonnes pratiques

Bulgarie : lorsque cela est possible, les organes de répression bulgares consultent activement les autorités de la Partie requise avant d'envoyer une requête. Ils coopèrent, par exemple, avec les autorités des États-Unis par l'intermédiaire des agents de liaison américains présents en Bulgarie et d'autres contacts spécialement désignés en matière de cybercriminalité.

République tchèque : l'autorité centrale et les autorités judiciaires tchèques consultent régulièrement leurs partenaires étrangers les plus fréquents. Dans les affaires complexes, cette consultation a lieu par écrit directement entre autorités responsables, par l'intermédiaire des réseaux de spécialistes de l'entraide judiciaire ou de réunions de coordination bilatérales ou multilatérales.

[25] Plusieurs États approuvent la pratique de consultation préalable mais sans indiquer *s'ils consultent eux-mêmes* d'autres États. Cependant, ils encouragent les autres États à les consulter (Arménie, Australie, Suisse).

[26] La Croatie, Chypre, la Finlande, la Géorgie, l'Islande, Israël, la Lettonie, le Luxembourg, le Panama, le Sri Lanka, « l'ex-République yougoslave de Macédoine », l'Ukraine et le Royaume-Uni n'ont pas répondu à cette question.

France : l'autorité centrale et les magistrats remplissant des fonctions de liaison engagent un dialogue constructif avec les autorités de la Partie requise. La France souligne que ces contacts informels visent à faciliter l'aide et ne doivent pas servir de filtre avant l'envoi d'une requête formelle.

Lituanie : les Parties requises sont généralement consultées avant l'envoi des requêtes, en particulier lorsque la Lituanie travaille avec un nouvel État partenaire ou lorsqu'il s'agit d'une requête sensible ou complexe.

Serbie : si nécessaire, la Serbie consulte préalablement la Partie requise avant de rédiger la requête complète pour assurer que toutes les mesures nécessaires pourront être prises et que toutes les preuves demandées pourront être recueillies.

Slovaquie : l'autorité compétente communique souvent avec le ministère américain de la Justice, même avant d'envoyer une demande de conservation. Par exemple, dans le cas des prestataires moins connus, l'autorité demande aux États-Unis l'adresse correcte du prestataire concerné ou un avis sur sa capacité à conserver des données.

2.14.3 Conclusion

La plupart des Parties déclarent qu'avant d'envoyer une demande formelle d'entraide judiciaire, elles consultent l'État requis, si nécessaire, par l'intermédiaire d'un mécanisme parmi plusieurs disponibles. Ces réponses ne semblent pas cohérentes avec les réclamations qui ont conduit à cette Recommandation. Il se peut que les États recourent maintenant plus fréquemment à des consultations préalables. Quoi qu'il en soit, des consultations préalables plus fréquentes permettront de réduire les erreurs, les dépenses, les retards, la perte de preuves et le travail inutile.

2.15 Rec. 15 – Transparence au sujet des conditions applicables, des seuils et des motifs de refus

> Les Parties devraient assurer la transparence en ce qui concerne les conditions applicables en matière de demandes d'entraide, et les raisons de refus, notamment pour les seuils concernant les affaires vénielles, sur les sites web des autorités centrales.

2.15.1 Aperçu général des suites données à la Recommandation

La consultation de sites web pour obtenir des informations essentielles est de plus en plus fréquente. C'est pourquoi les Parties ont suggéré qu'il serait utile, dans la mesure du possible, de publier les conditions applicables sur le web, dans l'intérêt des États requérants. La formation, les consultations, le travail de liaison et d'autres pratiques sont utiles mais ils n'atteignent pas nécessairement toutes les personnes pouvant être impliquées dans la rédaction d'une demande d'entraide judiciaire. Un site web peut atteindre un plus grand nombre de ces agents publics plus rapidement.

De nombreux États n'ont pas répondu à la suggestion de publier l'information essentielle relative à l'entraide judiciaire sur un site web.[27] Ils se contentent de citer ou de fournir des liens aux lois et

[27] La Croatie, Chypre, la Géorgie, l'Allemagne, la Hongrie, l'Islande, le Luxembourg, le Monténégro, le Panama, la Slovénie, le Sri Lanka, « l'ex-République yougoslave de Macédoine », l'Ukraine et le Royaume-Uni n'ont pas répondu à la question. La Bulgarie et Israël ont indiqué n'avoir aucune information nouvelle à fournir à ce sujet.

traités pertinents pour eux et/ou indiquent que les informations concernant chaque affaire, y compris les raisons de refus d'une requête, sont transmises confidentiellement à l'État requérant.

Néanmoins, de nombreux États publient en fait l'information essentielle relative à l'entraide judiciaire et/ou des liens à la législation et aux traités pertinents sur des sites publics ou à accès quelque peu restreint (Australie, Belgique[28], Canada, République tchèque, Italie,[29] Japon, Moldova, Pologne, Serbie, Espagne, Suisse, Turquie). D'autres envisagent de le faire (États-Unis, Finlande, Pays-Bas, République tchèque – publication d'informations plus détaillées qu'actuellement, Slovaquie). Lorsque cette information n'est publiée que dans la ou les langues nationales, son utilité pour les autres Parties reste limitée.

2.15.2 Exemples de bonnes pratiques

Canada : l'autorité centrale maintient un site web public détaillé qui fournit aux agents publics canadiens et étrangers des informations procédurales et de fond en vue de la rédaction d'une requête d'entraide judiciaire efficace. On trouve aussi sur ce site web des indications sur la manière de requérir une aide sur des questions mineures. Des guides pratiques et des modèles sont accessibles sur le site.

Japon : le site web du ministère de la Justice fournit des explications détaillées en anglais sur les conditions applicables aux demandes d'entraide judiciaire, y compris les motifs de refus.

Moldova : toutes les informations nécessaires sur les conditions applicables aux requêtes d'entraide judiciaire sont publiées sur le site web du Bureau du Procureur général. Ces informations sont actuellement publiées uniquement en moldave mais Moldova envisage de les faire traduire et de les publier également en anglais.

Turquie : l'autorité centrale fournit des informations générales et détaillées au sujet de l'entraide judiciaire sur son site web, qui permet aussi d'accéder à la législation turque régissant les pratiques d'entraide judiciaire.

2.15.3 Conclusion

Plusieurs États ne semblent pas être encore parvenus à héberger et maintenir un site web sur l'entraide judiciaire. Les États qui disposent d'un site à ce sujet devraient publier le plus d'informations générales possibles, notamment à propos de la législation applicable et des traités, ainsi que des modèles de formulaires, des guides et des outils en ligne par exemple, en s'abstenant de publier des informations portant sur des affaires spécifiques. La publication des procédures d'entraide judiciaire permettrait de réduire le volume de travail des agents publics concernés à toutes les étapes du processus de l'entraide judiciaire, aussi bien dans les États requis que dans les États requérants.

3 Période de conservation des données (Rec. 16)

> Le T-CY devrait faciliter une plus grande transparence vis-à-vis de la période de conservation des données suite à une demande de conservation étrangère conformément l'article 29 de la Convention de Budapest. Le T-CY devrait documenter les périodes de conservation.

[28] La Belgique publie cette information sur le site web du PC-OC.

[29] L'Italie utilise le site du Réseau judiciaire européen, qui n'est pas ouvert à toutes les Parties à la Convention de Budapest.

3.1 Durée de la période de conservation

Le tableau ci-dessous indique la durée des périodes de conservation des données et de leur renouvellement éventuel, telle qu'indiquée par les États :

Partie	Période de conservation des données suite à une demande étrangère	Conditions et période de prolongation ou de renouvellement de la conservation des données spécifiées
Albanie	90 jours	90 jours
Andorre	Aucune information n'a été fournie	Aucune information n'a été fournie
Arménie	Pas de limite spécifique	Aucune information n'a été fournie
Australie	L'article 3 du chapitre 3-1A de la loi sur les télécommunications (interception et accès) de 1979 dispose qu'un fournisseur est tenu de conserver les communications depuis le jour où il est notifié d'une demande étrangère jusqu'au jour où la Police fédérale australienne l'informe que cette demande est annulée. La Police fédérale australienne annule une demande de conservation si le pays étranger demandeur ne transmet pas au Procureur général une requête dans un délai de 180 jours.	Il n'existe pas de mécanisme d'extension ou de renouvellement de la période de conservation des données spécifiées. Le pays requérant doit remplir une nouvelle demande de conservation des données. La période effective de conservation de 180 jours excède les 60 jours minimum prévus à l'article 29.
Autriche	La conservation des données n'est pas soumise à une limite spécifique.	L'extension ou le renouvellement sont possibles sur demande de l'État requérant, en prenant en compte la proportionnalité de la mesure de conservation. Il n'est pas prévu de périodes ou de limites spécifiques.
Azerbaïdjan	Aucune information n'a été fournie	Aucune information n'a été fournie
Belgique	Aucune information n'a été fournie	Aucune information n'a été fournie
Bosnie-Herzégovine	L'harmonisation des dispositions du Règlement sur la conservation des fichiers et documents archivés sera nécessaire pour assurer que la période de conservation de tous les fichiers est conforme à celle prescrite par la Convention. La seule exception concernera les bases de données électroniques de l'autorité centrale qui seront conservées en permanence.	L'harmonisation des dispositions du Règlement sur la conservation des fichiers et documents archivés sera nécessaire pour assurer que la période de conservation de tous les fichiers est conforme à celle prescrite par la Convention. La seule exception concernera les bases de données électroniques de l'autorité centrale qui seront conservées en permanence.
Bulgarie	3 mois	L'extension de la période de conservation n'est pas autorisée
Canada	Aux termes de la loi sur la protection des Canadiens contre la cybercriminalité, le Canada peut conserver des données informatiques à la demande de la police	L'extension de la période de conservation n'est pas autorisée

Partie	Période de conservation des données suite à une demande étrangère	Conditions et période de prolongation ou de renouvellement de la conservation des données spécifiées
	ou sur l'ordre d'un tribunal. Dans un premier temps, la police canadienne adresse normalement une demande de conservation des données au maître du fichier. Le seuil légal requis pour une telle demande est l'existence de soupçons raisonnables que : - une infraction réprimée par la législation d'un État étranger a été ou va être commise ; - une enquête est conduite par une personne ou autorité chargée de l'instruction de ce type d'infraction dans l'État en question ; et, - les données informatiques détenues ou contrôlées par la personne ou l'entité visée par la demande seront utiles pour l'enquête. Les demandes de conservation sont valables pour une durée de 90 jours non renouvelable. Cependant, la police canadienne peut obtenir un ordre de conservation d'un tribunal canadien.	
Croatie	Aucune information n'a été fournie	Aucune information n'a été fournie
Chypre	Aucune information n'a été fournie	Aucune information n'a été fournie
République tchèque	La législation tchèque ne prévoit pas de limite pour la conservation de données au titre de l'article 29 de la Convention de Budapest. Néanmoins, la requête d'entraide judiciaire doit être envoyée le plus rapidement possible.	
Danemark	6 mois	L'extension de la période de conservation n'est pas autorisée
République dominicaine	La période prévue est de quatre-vingt-dix (90) jours.	La période de conservation est renouvelable à tout moment sur demande pour un nombre de jours identique.
Estonie	La conservation des données peut être obtenue très rapidement, si possible pendant une journée.	Les pouvoirs généraux s'appliquent à la conservation des données. La législation ne prévoit pas de conditions ou de périodes supplémentaires.
Finlande	Aucune information n'a été fournie	Aucune information n'a été fournie
France	90 jours	90 jours
Géorgie	Aucune information n'a été fournie	Aucune information n'a été fournie
Allemagne	Si des données sont saisies suite à une demande de conservation rapide, elles peuvent être conservées pendant	Voir colonne de gauche.

Partie	Période de conservation des données suite à une demande étrangère	Conditions et période de prolongation ou de renouvellement de la conservation des données spécifiées
	la durée raisonnablement nécessaire pour l'enquête et, si une procédure judiciaire est ouverte, pendant la durée nécessaire pour établir les preuves.	
Hongrie	3 mois	Aucune information n'a été fournie
Islande	Aucune information n'a été fournie	Aucune information n'a été fournie
Israël	La législation israélienne autorise la conservation des données pour une période de six mois, sur décision d'un juge.	Un juge peut étendre la période de conservation à plus de six mois, sous certaines conditions fixées par lui, en réponse à une demande spécifique. En pratique, le tribunal prend en compte le degré d'atteinte à la vie privée de l'individu soupçonné et de tiers au regard de l'intérêt de l'enquête.
Italie	90 jours	6 mois
Japon	60 jours	En cas de conservation des données sur la base de la coopération volontaire des FSI, la période de conservation peut dépasser 60 jours.
Lettonie	30 jours	90 jours maximum
Liechtenstein	La conservation des données n'est pas soumise à une limite spécifique.	Il n'est pas prévu de périodes ou de limites spécifiques.
Lituanie	Aux termes de la Loi sur les communications électroniques, les fournisseurs de services sont tenus de conserver les données pendant 6 mois, avec possibilité de renouvellement pour une nouvelle période de 6 mois.	Aucune condition spécifique n'est requise pour étendre ou renouveler la période de conservation. Une demande de renouvellement suffit.
Luxembourg	Aucune information n'a été fournie	Aucune information n'a été fournie
Malte	Conservation des données de communications relatives à l'accès à l'Internet et au courrier électronique pendant une période de six mois à partir de la date de la communication. Conservation des données de communications relatives au réseau de téléphonie fixe, au réseau de téléphonie mobile et au réseau internet pendant un an à partir de la date de la communication.	
Maurice	Le temps jugé raisonnablement nécessaire pour enquêter sur une	Les conditions et la période d'extension ou de renouvellement sont régies par les

Partie	Période de conservation des données suite à une demande étrangère	Conditions et période de prolongation ou de renouvellement de la conservation des données spécifiées
	infraction ; en cas d'institution de poursuites, jusqu'à la conclusion de l'affaire ; ou encore la durée fixée par un juge dans une ordonnance.	dispositions de l'article 11(3) de la loi sur la cybercriminalité (CMCA).
Moldova	1 mois	Jusqu'à six mois
Monténégro	La législation ne prévoit pas de limite spécifique	
Pays-Bas	90 jours	90 jours
Norvège	90 jours Si les données sont conservées sur demande internationale, il n'est pas nécessaire de renouveler la période de conservation car celle-ci est généralement étendue par les autorités norvégiennes.	
Panama	Aucune information n'a été fournie	Aucune information n'a été fournie
Philippines	6 mois	Une demande unique de prolongation pour une période de conservation de six mois peut être acceptée en vertu de la loi de la République n° 10175.
Pologne	Si les données sont conservées au titre d'une requête internationale, il n'est pas nécessaire de renouveler la période de conservation.	
Portugal	3 mois	Un an maximum
Roumanie	60 jours	30 jours
Serbie	Pas de législation sur la conservation des données	
Slovaquie	90 jours	90 jours
Slovénie	Pas de législation sur la conservation des données	
Espagne	90 jours	90 jours
Sri Lanka		
Suisse	90 jours	Les demandes de conservation des données peuvent être prolongées ou renouvelées à tout moment dans le délai exigé pour la soumission d'une demande formelle d'entraide judiciaire.
« L'ex-République yougoslave de Macédoine »	Aucune information n'a été fournie	Aucune information n'a été fournie
Turquie	Bien que l'article 29(7) de la Convention de Budapest exige des Parties qu'elles conservent les données pendant au moins 60 jours, il n'existe pas de dispositions spécifiques sur les	

Partie	Période de conservation des données suite à une demande étrangère	Conditions et période de prolongation ou de renouvellement de la conservation des données spécifiées
	demandes de conservation et la durée de la période de conservation. Cependant, l'article 8(1)(c) de la loi n° 6706, intitulé « Requête judiciaire étrangère », réglemente la conservation des preuves, y compris la conservation temporaire de données, pendant une période de 40 jours. Si la demande est reçue dans l'intervalle des 40 jours, la période de conservation des données est prolongée. Les données de trafic sont également conservées pendant une certaine période au titre de la loi n° 5651. Aux termes de l'article 5(3) de la loi n° 5651, les fournisseurs de services sont tenus de conserver les données de trafic de leurs services d'hébergement pendant au moins un an et deux ans maximum, conformément aux durées indiquées dans la réglementation ; ils doivent aussi assurer l'exactitude, l'intégrité et la confidentialité de ces données. En vertu de l'article 6(1)(b) de la loi n° 5651, les fournisseurs d'accès sont tenus de conserver les données de trafic de leurs services pendant au moins six mois et deux ans maximum, conformément aux durées indiquées dans la réglementation ; ils doivent aussi assurer l'exactitude, l'intégrité et la confidentialité de ces données.	
Ukraine	Aucune information n'a été fournie	Aucune information n'a été fournie
Royaume-Uni	Aucune information n'a été fournie	Aucune information n'a été fournie
États-Unis d'Amérique	90 jours	90 jours

3.2 Aperçu général des suites données à la Recommandation

Le T-CY est conscient du fait que les différentes modalités d'application des mesures de conservation peuvent être source de confusion et de problèmes pour les États requérants. De plus, il est souvent difficile de traiter et de mener à bien une requête d'entraide judiciaire avant que s'achève la période de conservation des données, en particulier lorsque l'enquête continue à évoluer ou lorsque des raisons pratiques – délais de traduction, par exemple – entraînent des retards. Cette Recommandation a pour but de permettre aux États requérants de déterminer s'ils peuvent raisonnablement compter sur les données qu'ils cherchent à obtenir.

Les réponses des États à cette question se répartissent globalement en deux catégories selon qu'ils ont défini une période spécifique de conservation des données, ainsi que des conditions de renouvellement de cette période, ou qu'ils n'ont établi aucune limite de durée spécifique, souvent parce qu'ils ne disposent pas d'un texte de loi écrit régissant cette question.[30]

La durée de la période de conservation des données varie en outre quelque peu parmi les États qui ont établi une limite à ce sujet. La majorité, cependant, ont opté pour une période plus longue :

- seul quelques États prévoient une période de 60 jours ou moins (Japon, Lettonie, Roumanie) ;
- la plupart ont opté pour une période de 90 jours (Albanie, Bulgarie, Canada, Espagne, États-Unis, France, Hongrie, Italie, Pays-Bas, Portugal, Slovaquie) ou de 180 jours (Australie, Danemark, Lituanie, Malte).

Dans certains États, la durée de la période de conservation des données varie en fonction de la demande du procureur ou de l'État étranger concerné ou bien cette durée n'est pas spécifiquement limitée (Arménie, Autriche, Estonie, Maurice, Monténégro, Pologne, République tchèque, Serbie, Slovénie, Suisse) et, le cas échéant, les données peuvent donc être conservées indéfiniment.

Les fournisseurs de services internet peuvent décider de conserver les données pendant une période plus longue que celle exigée par la législation pertinente.

La plupart des États autorisent le renouvellement de la période de conservation des données (parfois en exigeant une nouvelle requête formelle). Seuls la Bulgarie et le Japon déclarent qu'ils ne l'autorisent pas. Les États limitent parfois la durée totale de conservation des données, y compris en cas de renouvellement de la période initiale. Lorsqu'une telle limite existe, elle se situe presque toujours entre six mois et deux ans (Albanie, Australie, Canada, Espagne, États-Unis, France, Italie, Lituanie, Malte, Maurice, Pays-Bas, Portugal).

3.3 Conclusion

Des périodes plus longues visent à assurer la conservation des données pendant que les Parties préparent leurs requêtes d'entraide judiciaire. Pour ce faire, une période initiale assez longue, associée à la possibilité de renouveler facilement cette période ou de conserver indéfiniment les données, est nécessaire. Pour éviter les erreurs à ce sujet, les Parties devraient vérifier au préalable auprès de leurs partenaires étrangers les conditions exactes de conservation des données. Il serait également utile que les Parties facilitent l'accès à toutes les informations relatives à la conservation des données.

4 Recommandations 17 et 18

4.1 Rec. 17 – Formulaires plurilingues

> Rec. 17 – Le Conseil de l'Europe devrait – de par ses projets de renforcement des capacités – élaborer ou créer des liens vers des formulaires modèles standardisés, plurilingues pour les demandes au titre de l'article 31.

[30] L'Azerbaïdjan, la Belgique, la Croatie, Chypre, la République dominicaine, la Finlande, la Géorgie, l'Islande, le Luxembourg, la Moldova, le Panama, le Sri Lanka, « l'ex-République yougoslave de Macédoine », l'Ukraine et le Royaume-Uni n'ont pas répondu à cette question.

4.1.1 Suites données à la Recommandation

Dans le cadre du projet Cybercrime@EAP II, le Conseil de l'Europe a mis au point en 2016 des projets de formulaires types de demande de conservation des données à utiliser dans les requêtes au titre des articles 29 et 30 de la Convention de Budapest et dans les demandes de données informatiques (informations sur les abonnés, données de trafic, données sur le contenu) adressées au titre de l'article 31 de la Convention de Budapest.

Ces formulaires types ont été développés lors d'activités menées avec les États du Partenariat oriental (Arménie, Azerbaïdjan, Belarus, Géorgie, Moldova et Ukraine), avec le soutien d'experts de France, d'Allemagne, du Portugal, de « l'ex-République yougoslave de Macédoine » et du Royaume-Uni.

Le formulaire type de demande de conservation de données aurait été testé en pratique par la Géorgie et la Moldova. La France a adapté et modifié le formulaire type en vue de son utilisation concrète.

Dans ces formulaires types, la part du texte est limitée ; ils contiennent principalement des cases à cocher. Cela facilitera leur conversion en formulaire plurilingue.

Pendant des années, la Slovaquie a utilisé un formulaire pour les demandes de conservation rapide de données au titre de l'article 29, en particulier pour les demandes adressées aux États-Unis.

4.1.2 Conclusion

Des progrès positifs ont été réalisés dans la mise au point des modèles de formulaires.

Il est recommandé que des experts du T-CY examinent ces modèles de formulaires et les communiquent ensuite au T-CY, aux points de contact 24/7 et aux autorités d'entraide judiciaire pour commentaires.

4.2 Rec. 18 – Ressources en ligne

> Rec. 18 – Le Conseil de l'Europe devrait explorer la possibilité d'établir un fonds de ressources en ligne contenant des informations sur les systèmes de droit interne des Parties concernant les preuves électroniques et la cybercriminalité, ainsi que les seuils légaux, les conditions applicables aux preuves et autres qui doivent être remplis pour obtenir la communication de données informatiques stockées en vue de leur utilisation devant les tribunaux.

4.2.1 Suites données à la Recommandation

La Division de cybercriminalité du Secrétariat (Secrétariat du T-CY et Bureau du Programme du Conseil de l'Europe sur la cybercriminalité, C-PROC) a commencé à mettre sur pied la Communauté Octopus sur la cybercriminalité en 2014, y compris un outil consacré à la coopération internationale.

Les progrès accomplis en ce domaine ont été présentés au T-CY 14 les 1-2 décembre 2015 et le T-CY a salué « la création de la Communauté Octopus sur la cybercriminalité, en appelant les membres et les observateurs du T-CY à contribuer à l'élaboration des outils mis à disposition sur cette plateforme ».

En 2016, le Secrétariat a sollicité les données nécessaires des Parties à la Convention. Les données reçues ont été téléchargées. En avril 2017, sur 54 Parties, 16 avaient fourni des informations complètes, 21 avaient fourni des informations partielles ou incomplètes et 17 n'avaient pas encore contribué à la Communauté Octopus.

Certains facteurs techniques empêchent encore de faire de cet outil une application facile à utiliser, notamment des capacités insuffisantes en termes de contenus, le manque de flexibilité du système de gestion des contenus qui nuit à l'expérience des usagers, ainsi que les questions d'accessibilité et de sécurité de la plateforme. Le Secrétariat du T-CY examine actuellement des propositions de sous-traitance de la Communauté Octopus afin de surmonter les problèmes techniques et de permettre à la Communauté de continuer à évoluer.

4.2.2 Conclusion

Des progrès importants ont été réalisés dans la mise en place d'un outil qui, une fois pleinement opérationnel, apportera beaucoup à la coopération internationale en matière de cybercriminalité et de preuves électroniques.

Les Parties sont invitées à fournir au Secrétariat du T-CY les données nécessaires pour compléter l'information concernant leurs autorités et procédures respectives. Des efforts supplémentaires devraient être engagés pour assurer la mise à disposition d'informations complètes sur toutes les Parties.

Compte tenu des capacités internes limitées pour résoudre les problèmes techniques et soutenir la poursuite du développement de la Communauté Octopus, l'option de sous-traitance devrait être poursuivie. Les Parties et les donateurs devraient envisager le versement de contributions volontaires pour soutenir l'évolution continue de la Communauté Octopus.

5 Conclusions, recommandations et suivi

5.1 Conclusions

- L'entraide judiciaire est et restera l'un des principaux moyens de recueillir des preuves électroniques dans les procédures pénales. Tout en recherchant de nouvelles solutions pour les cas où l'entraide judiciaire n'est pas une option, les États doivent prendre les mesures nécessaires pour améliorer l'efficience de l'entraide judiciaire lorsqu'elle peut être obtenue. Les suites données aux Recommandations adoptées par le T-CY en décembre 2014 contribueront à la réalisation de cet objectif.

- Le T-CY se réjouit du fait que 40 Parties et Observateurs ont communiqué de nombreuses informations sur les suites données à ces Recommandations. Le Comité note cependant que, dans certains cas, des compléments d'information seraient utiles pour comprendre pleinement la situation factuelle et juridique dans un pays. Le T-CY regrette que certaines Parties n'aient pas répondu au questionnaire.

- Les informations reçues montrent que de nombreux États ont donné suite à un grand nombre des Recommandations. Il existe, pour toutes les Recommandations, des bonnes pratiques qui pourraient servir d'exemple pour les autres États.

- Les informations reçues donnent parfois une image assez optimiste du fonctionnement de l'entraide judiciaire. Les États déclarent qu'ils s'efforcent de s'assurer que leurs requêtes d'entraide judiciaire sont exactes et complètes mais s'inquiètent du fait qu'il n'en va pas de même pour les requêtes qu'ils reçoivent. Cela laisse à penser qu'il serait

nécessaire que le T-CY engage des efforts supplémentaires pour suivre le fonctionnement de l'entraide judiciaire dans la pratique.

- De nombreux États déclarent tenir des statistiques sur la cybercriminalité et les preuves électroniques aux fins de l'entraide judiciaire. Il serait utile que les États partagent ces données avec le T-CY.

5.2 Recommandations

Les suites supplémentaires à donner aux Recommandations adoptées par le T-CY sont décrites ci-dessous :

Rec. 1 Les Parties devraient pleinement mettre en œuvre et appliquer les dispositions de la Convention de Budapest sur la cybercriminalité, y compris les pouvoirs en matière de conservation des données (suite au rapport d'évaluation de 2012 du T-CY). [31]

Autres suites à donner à la Recommandation :

- ► Les Parties devraient poursuivre leurs efforts en vue de mettre en œuvre pleinement toutes les dispositions de la Convention de Budapest, y compris les dispositions internes qui ont une incidence sur la coopération internationale.
- ► Les Parties devraient supprimer les obstacles à l'exécution des demandes internationales de conservation des données au titre de l'article 29 – en particulier eu égard aux requêtes d'entraide judiciaire – et par ailleurs améliorer leur mise en œuvre au niveau national.
- ► Les Parties devraient engager les réformes nécessaires pour introduire dans leur législation nationale des dispositions spécifiques sur la conservation des données, comme recommandé par le T-CY dans les rapports d'évaluation sur la mise en œuvre rapide des dispositions de la Convention en matière de conservation des données.[32]

Rec. 2 Les Parties devraient envisager de tenir des statistiques ou d'établir d'autres mécanismes pour suivre l'efficience du processus d'entraide en ce qui concerne la cybercriminalité et les preuves électroniques.

Autres suites à donner à la Recommandation :

- ► Les Parties devraient communiquer des statistiques et des études de cas au Secrétariat du T-CY pour permettre l'évaluation continue par le T-CY du fonctionnement de l'entraide judiciaire en ce qui concerne la cybercriminalité et les preuves électroniques. Le T-CY devrait faciliter l'échange de bonnes pratiques pour encourager les Parties à tenir des statistiques.

Rec. 3 Les Parties devraient envisager, pour l'entraide, d'affecter davantage de personnel et du personnel plus formé aux technologies, non seulement au niveau central mais aussi au niveau des institutions responsables de l'exécution des demandes (comme les Bureaux locaux des procureurs).

---

[31] Chypre, la Géorgie, l'Islande, le Luxembourg, le Panama, le Sri Lanka, « l'ex-République yougoslave de Macédoine », l'Ukraine et le Royaume-Uni n'ont pas répondu à cette question.

[32] Rapport d'évaluation « Mise en œuvre des dispositions de la Convention de Budapest en matière de conservation des données »
https://rm.coe.int/16802e722f
Rapport d'évaluation supplémentaire sur la mise en œuvre des dispositions de la Convention de Budapest en matière de conservation (anglais uniquement)
https://rm.coe.int/168044be2b

Autres suites à donner à la Recommandation :

- ► Les États devraient poursuivre et envisager d'intensifier leurs efforts en vue d'affecter du personnel formé aux technologies aux fins de l'entraide judiciaire, pour assurer l'efficience des procédures au niveau du centre et des régions.

Rec. 4 Les Parties devraient envisager de dispenser une meilleure formation pour renforcer l'entraide, la coopération policière et d'autres formes de coopération internationale en matière de cybercriminalité et de preuves électroniques. La formation et l'échange d'expériences devraient en particulier viser les procureurs et les juges et encourager une coopération directe entre autorités judiciaires. Une telle formation devrait être soutenue par les programmes de consolidation de capacités du Conseil de l'Europe et d'autres organisations.

Autres suites à donner à la Recommandation :

- ► Les États devraient examiner la possibilité d'adopter une approche systématique de la formation à l'entraide judiciaire et à d'autres formes de coopération internationale en matière de cybercriminalité et de preuves électroniques.
- ► Le Conseil de l'Europe (Secrétariat du T-CY ou C-PROC) devrait établir une liste des formateurs et des institutions capables de fournir une formation standardisée et reproductible à la coopération internationale en matière de cybercriminalité et de preuves électroniques.

Rec. 5 Les Parties et le Conseil de l'Europe devraient travailler à renforcer le rôle des points de contact 24/7 conformément à l'article 35 de la Convention de Budapest, notamment :

g. veiller, conformément à l'article 35.3 de la Convention de Budapest, à disposer de personnel formé et équipé pour faciliter le travail opérationnel et conduire ou soutenir des activités liées à l'entraide ;
h. veiller à ce que les points de contact promeuvent activement leur rôle parmi les autorités nationales et leurs homologues étrangères ;
i. assurer entre les Parties des réunions régulières et la formation du réseau 24/7 ;
j. encourager les autorités compétentes et les points de contact 24/7 à envisager des procédures de suivi pour superviser le traitement des demandes basées sur l'article 31 et faire un retour d'information à l'État requérant ;
k. établir, dans la mesure du possible, des points de contact (supplémentaires) dans les services de poursuite pour permettre un rôle plus direct en matière d'entraide et une réponse plus rapide aux demandes ;
l. faire jouer aux points de contact 24/7 un rôle de soutien pour les demandes « article 31 ».

Suites à donner à la Recommandation :

- ► Les États devraient prendre de nouvelles mesures pour améliorer la coopération entre les points de contact 24/7 et les autorités chargées de l'entraide judiciaire.
- ► Le T-CY devrait discuter de cas concrets impliquant des points de contact 24/7 afin de résoudre les problèmes existants.
- ► Le Conseil de l'Europe devrait organiser des ateliers ou des sessions de formation pour les points de contact 24/7 créés conformément à l'article 35 pour faciliter le fonctionnement du réseau.

Rec. 6 Les Parties devraient envisager une rationalisation des procédures et réduire le nombre d'étapes requises pour les demandes d'entraide au niveau national. A cet égard, les Parties doivent partager les bonnes pratiques avec le T-CY.

Suites à donner à la Recommandation :

- ► Les États devraient examiner la possibilité d'adopter – en s'appuyant sur l'expérience d'autres États – de nouvelles mesures pour réduire le nombre d'étapes requises pour l'entraide judiciaire.

Rec. 7 Les Parties devraient utiliser tous les canaux disponibles pour la coopération internationale. Ceci peut inclure l'entraide judiciaire formelle, la coopération policière et d'autres.

Suites à donner à la Recommandation :

- ► Les États devraient envisager de développer de nouveaux canaux de coopération informels dans les limites autorisées par la législation pertinente.

Rec. 8 Les Parties sont encouragées à établir des procédures d'urgence pour les demandes liées aux risques pour la vie et à des circonstances extrêmes similaires. Le T-CY devrait documenter les pratiques des Parties et des fournisseurs de service.

Suites à donner à la Recommandation :

- ► Les États devraient sensibiliser les décideurs à l'augmentation du nombre de situations dans lesquelles une procédure d'urgence est requise pour permettre la divulgation rapide de preuves électroniques. Les projets de renforcement des capacités du Conseil de l'Europe devraient faciliter la sensibilisation des décideurs à ce sujet.
- ► Les États devraient améliorer et formaliser les procédures d'urgence concernant la divulgation de preuves électroniques.
- ► L'introduction de dispositions relatives aux procédures d'urgence nécessitant des mesures préventives – via l'entraide judiciaire et la coopération directe avec les fournisseurs de données – devrait en outre être envisagée dans l'élaboration du Protocole à la Convention de Budapest.

Rec. 9 Les Parties devraient accuser réception des demandes systématiquement et notifier, sur demande, les actions prises.

Suites à donner à la Recommandation :

► Les points de réception des requêtes d'entraide judiciaire devraient systématiquement en accuser réception et indiquer la personne à contacter pour le suivi.

Rec. 10 Les Parties devraient envisager l'ouverture d'une enquête nationale sur demande étrangère ou information spontanée pour faciliter le partage d'information ou accélérer l'entraide.

Suites à donner à la Recommandation :

- ► Les États devraient fournir des informations supplémentaires sur la mise en œuvre de cette Recommandation, y compris l'utilisation de l'information spontanée (article 26 de la Convention de Budapest).

Rec. 11 Les Parties devraient utiliser la transmission électronique des demandes conformément à l'article 25.3 de la Convention de Budapest relatif aux moyens rapides de communication.

Suites à donner à la Recommandation :

- ► Les États devraient supprimer les obstacles à la transmission électronique des demandes.

Rec. 12 Les Parties devraient veiller à ce que les demandes soient spécifiques et contiennent toutes les informations nécessaires.

Suites à donner à la Recommandation :

- ► Les États devraient communiquer au T-CY des exemples de difficultés causées par des requêtes d'entraide judiciaire inadéquates. Cela permettrait de mettre en regard le point de vue des États au sujet des demandes reçues et envoyées.

Rec. 13 Conformément à l'article 25.5 de la Convention de Budapest et au paragraphe 259 du Rapport explicatif, les Parties sont encouragées à faire preuve de flexibilité lorsqu'elles appliquent la double incrimination pour faciliter l'octroi de l'aide.

Suites à donner à la Recommandation :

- ► Les États devraient continuer à faire preuve de flexibilité dans l'application des normes de double incrimination, conformément à la Convention.

Rec. 14 Les Parties sont encouragées à consulter les autorités de la Partie requise avant d'envoyer les demandes, quand cela est nécessaire.

Suites à donner à la Recommandation :

- ► Les États devraient recourir plus fréquemment à l'option consistant à consulter au préalable les autorités de la Partie requise, afin de réduire au minimum les erreurs, les retards et les coûts.

Rec. 15 Les Parties devraient assurer la transparence en ce qui concerne les conditions applicables en matière de demandes d'entraide, notamment pour les seuils concernant les affaires vénielles, sur les sites Web des autorités centrales.

Suites à donner à la Recommandation :

- ► Les États devraient engager des efforts supplémentaires pour mettre en œuvre cette Recommandation. Ils devraient aussi s'appuyer sur la Communauté Octopus à cet égard.

Rec. 16 Le T-CY devrait faciliter une plus grande transparence vis-à-vis de la période de conservation des données suite à une demande de conservation étrangère conformément l'article 29 de la Convention de Budapest. Le T-CY devrait documenter les périodes de conservation.

Suites à donner à la Recommandation :

- ► Les Parties devraient assurer l'accès facile aux renseignements relatifs à la période de conservation des données et à d'autres conditions sur leurs sites web concernant l'entraide judiciaire, ainsi que via la Communauté Octopus.
- ► Le T-CY considère qu'une période de conservation des données de moins de 90 jours, sans possibilité de renouvellement au moins une fois, n'est pas suffisante.

Rec. 17 — Le Conseil de l'Europe devrait — de par ses projets de renforcement des capacités — élaborer ou créer des liens vers des formulaires modèles standardisés, plurilingues pour les demandes au titre de l'article 31.

Suites à donner à la Recommandation :

- ► Des experts sélectionnés parmi les membres du T-CY devraient passer en revue les modèles préparés dans le cadre des projets de renforcement des capacités,

puis les communiquer au T-CY, aux points de contact 24/7 et aux autorités d'entraide judiciaire pour commentaires et adoption.

- Les modèles devraient ensuite être finalisés et mis à la disposition des Parties via la Communauté Octopus.

Rec. 18 – Le Conseil de l'Europe devrait explorer la possibilité d'établir un fonds de ressources en ligne contenant des informations sur les systèmes de droit interne des Parties concernant les preuves électroniques et la cybercriminalité, ainsi que les seuils légaux, les conditions applicables aux preuves et autres qui doivent être remplis pour obtenir la communication de données informatiques stockées en vue de leur utilisation devant les tribunaux.

Suites à donner à la Recommandation :

- Les Parties devraient fournir les informations requises via l'outil en ligne sur la coopération internationale de la Communauté Octopus.
- Le Conseil de l'Europe devrait envisager de sous-traiter la Communauté Octopus pour résoudre certains problèmes techniques et favoriser la poursuite de l'évolution de ses outils. Les Parties et les donateurs devraient réfléchir à la possibilité de verser des contributions volontaires à cette fin.

5.3 Suivi

Le partage d'affaires, d'expériences et d'observations concernant l'entraide judiciaire et d'autres formes de coopération internationale devrait devenir un élément régulier des sessions plénières du T-CY.

Les Parties et les Observateurs sont invités à notifier le T-CY des suites données aux Recommandations au cours des sessions plénières.

_____

6 Annexe : suites données à la Recommandation du T-CY sur l'entraide judiciaire au moyen d'activités de renforcement des capacités

Le Bureau du Programme du Conseil de l'Europe sur la cybercriminalité (C-PROC), sis à Bucarest, Roumanie et opérationnel depuis avril 2014, a pour vocation d'aider les pays du monde entier dans la mise en œuvre de la Convention de Budapest, y compris les suites données aux recommandations du T-CY.

Au mois d'août 2017, les projets en cours étaient les suivants :

Intitulé du projet	Région	Durée	Budget	Financement
Cybercrime@Octopus (numéro 3021)	Monde entier	Janvier 2014 - décembre 2019	3,5 millions d'EUR	Contributions volontaires (Estonie, Hongrie, Japon, Monaco, Roumanie, Slovaquie, Royaume-Uni, USA et Microsoft) [pas encore financées en intégralité]
Cybercrime@EAP II, projet sur la coopération internationale dans les pays du Partenariat Oriental (numéro 3271)	Arménie, Azerbaïdjan, Belarus, Géorgie, Moldova, Ukraine	Mai 2015 - décembre 2017	800 000 EUR	Projet conjoint UE/CdE (Partenariat pour une bonne gouvernance)
Cybercrime@EAP III, projet sur la coopération public-privé dans les pays du Partenariat Oriental (numéro 3608)	Arménie, Azerbaïdjan, Belarus, Géorgie, Moldova, Ukraine	Décembre 2015 - décembre 2017	1 200 000 EUR	Projet conjoint UE/CdE (Partenariat pour une bonne gouvernance)
GLACY+, projet d'Action Globale sur la Cybercriminalité Élargie (numéro 3148)[33]	Monde entier (pays noyaux ou prioritaires : République dominicaine, Ghana, Maurice, Maroc, Philippines, Sénégal, Sri Lanka, Tonga	Mars 2016 - février 2020	10 millions d'EUR	Projet conjoint UE/CdE
iPROCEEDS, projet de coopération internationale en matière de lutte contre la cybercriminalité en Europe du sud-est et en Turquie (3156)	Albanie, Bosnie-Herzégovine, Kosovo[34], Monténégro, Serbie, « l'ex-République yougoslave de Macédoine », Turquie.	Janvier 2016 - juin 2019	5,56 millions d'EUR	Projet conjoint UE/CdE

[33] Ce projet a été précédé de GLACY (Global Action on Cybercrime, de novembre 2013 à octobre 2016).
[34] *Cette désignation est sans préjudice des positions sur le statut et est conforme à la résolution 1244 du Conseil de sécurité et à l'avis de la CIJ sur la déclaration d'indépendance du Kosovo.

CyberSouth, projet de coopération en matière de cybercriminalité dans la région du Voisinage Sud (3692)	Algérie, Jordanie, Liban, Maroc, Tunisie	Juillet 2017 - juin 2020	3,35 millions d'EUR	Projet conjoint UE/CdE